Maîtrise des risques dans les systèmes de transport : proposition d'une nouvelle approche de modélisation dynamique

Dominique Legros

ED n°84 : SCIENCES ET TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

N° attribué par la bibliothèque
|__|__|__|__|__|__|__|__|__|__|__|

T H E S E

pour obtenir le grade de

DOCTEUR DE L'ECOLE NATIONALE SUPERIEURE DES MINES DE PARIS

Spécialité "Informatique temps réel, robotique et automatique "

présentée et soutenue publiquement par
Dominique LEGROS

le 29 décembre 2009

Maîtrise des risques dans les systèmes de transport :
Proposition d'une nouvelle approche de modélisation dynamique

Directeur de thèse : Tullio Joseph TANZI

Jury

M. Jacques LABETOULLE	Président
M. Alexis BONNECAZE	Rapporteur
M. Nicolas PUECH	Rapporteur
M. Jean Paul MARMORAT	Examinateur
M. Yves ROUCHALEAU	Examinateur
M. Jacques RAPHEL	Invité

Risk Management for Transportation Systems:

proposal for a new way for modelling dynamic systems

Ph D dissertation

To Chauncey STARR (1912/2007)

Résumé

A partir de la définition d'un paradigme espaces – processus énonçant que tout système peut se définir comme une combinaison espaces – processus, les espaces contenant toutes les conditions et moyens nécessaires à l'achèvement du processus, le travail proposé définit une approche modélisatrice permettant de conserver une démarche purement systémique depuis l'identification des concepts du système jusqu'au modèle de représentation.

Ce paradigme exprimant simplement qu'un système peut être vu à travers le comportement des différentes propriétés des entités intervenantes, le mémoire va proposer une représentation unifiée de la propriété permettant la manipulation conceptuelle et sémantique.

Une forme de représentation des comportements des propriétés sera ensuite proposée. Cette représentation sera définie à partir de l'expression d'un comportement sous forme d'expressions rationnelles; ces expressions étant elles-mêmes des suites de symboles représentatives des propriétés du système observé. Le mémoire montrera comment la forme de représentation proposée permet de retranscrire et d'exploiter simplement les comportements observés ou observables.

Le mémoire montrera comment manipuler ces éléments et quelles propriétés s'en dégagent. En particulier, le premier objectif de ce travail est une application à la maîtrise des risques systèmes, on exploitera donc le modèle dans la recherche et l'identification de situations dangereuses mais aussi pour la capacité d'évaluation des critères d'occurrence par un transfert de l'espace de propriétés vers un espace de probabilités.

Summary

From the definition of a new paradigm expressing that any system can be defined as a combination Spaces – Processes the proposed work defines a new system modelling aiming to preserve a purely systemic approach since the identification of concepts down to the model.

This paradigm basically expressing that a system can be seen through the behaviour of various properties of its entities; a system being a space containing all the conditions and the necessary means in completion of processes.

The dissertation proposes an unified representation of properties allowing their abstract and semantic manipulation.

A particular structure of dynamics of systems will be then proposed. This structure based on regular expressions as an ordered set of symbols representatives of properties of systems. The dissertation will show how to use these particular forms to simply and usefully describe systems behavior.

The dissertation will show how to manipulate these items and which properties get out of it. The first aim of this work being an application in risks management, operation of the model to find out and to identify dangerous situations but also the capability in evaluating occurrence criteria will be assumed.

Remerciements

Les travaux présentés dans ce mémoire ont été réalisés au Centre de Mathématiques Appliquées de l'Ecole Nationale Supérieure des Mines de Paris. Je tiens à manifester mon immense reconnaissance à Messieurs Yves ROUCHALEAU et Jean Paul MARMORAT professeurs pour leur encadrement et leur soutien indéfectible tout au long de ces travaux de recherche.

Je tiens à adresser tous mes remerciements à Monsieur Tullio Joseph TANZI, professeur à l'Ecole Nationale Supérieure des Télécommunications de Paris pour avoir dirigé cette thèse.

J'exprime ma profonde gratitude à Monsieur Nicolas PUECH, ingénieur diplômé de l'Ecole Nationale Supérieure des Télécommunications, agrégé de Mathématiques et Professeur en informatique, ainsi qu'à Monsieur Alexis BONNECAZE, professeur à l'Université de la Méditerranée qui m'ont fait l'honneur d'être rapporteurs de ce mémoire.

Je remercie également Monsieur Jacques LABETOULLE, professeur à l'Ecole Nationale Supérieure des Télécommunications pour avoir accepté de présider mon jury et Monsieur Jacques RAPHEL, Ingénieur de la Société Véolia Transport pour avoir répondu positivement à l'invitation à participer à ce jury.

Je ne remercierai jamais assez Messieurs François MELONIO, directeur général de COTEBA, Joël DIAZ DAS ALMAS, directeur de la division transports de COTEBA et Guy HAYS, directeur de la maîtrise d'œuvre du tramway de Nice, pour avoir aménager mon temps de travail au moment où les travaux de cette thèse le réclamaient, et ce, malgré les contraintes que ces facilités imposaient à la société.

J'adresse également tous mes remerciements à l'ensemble des personnes qui ont de près ou de loin participé aux travaux de cette thèse. Je pense notamment à Alexis pour l'aide précieuse et le soutien permanent qu'il m'a apporté mais aussi à Georges, Jacques, Alain, Bertrand, Luc, Emmanuel, Daniel, Claude, Jean Luc et Michel, à l'ensemble des traminots de Nice et à tout le personnel d'ALSTOM TGS Vitrolles anciennement INNORAIL.

Je manifeste ma gratitude à l'immense réseau des professionnels du transport qui en France et dans le monde collaborent pour que ces systèmes soient de plus en plus performants et continuent de fonctionner avec le même niveau de sûreté. C'est à travers toutes les rencontres et collaborations professionnelles que j'ai pu acquérir l'expérience dans laquelle cette thèse plonge une partie importante de ses racines.

Je remercie chaleureusement mes amis Olivier, Patrice et Patrick et ma famille et ma belle famille pour leur soutien et leur affection pendant toute cette tranche de vie que fut la préparation de ce mémoire.

Enfin, je dédie ce mémoire à Catherine, à Timothée et à Grégoire qui au-delà de leur affection et de leur compréhension ont sacrifié certains jours de repos hebdomadaire et certaines vacances lorsque cette thèse l'imposait.

SOMMAIRE

TABLE DES FIGURES

INTRODUCTION

Il est difficile de parler de sécurité des systèmes de transport sans se référer au transport ferroviaire car il est vrai que celui-ci représente une des plus vieilles cultures de la sécurité. Des premières lignes françaises à traction animale en 1827 aux premières voitures de voyageurs en 1832, le chemin de fer s'est rapidement imposé comme un mode de transport attractif. Cependant, compte tenu des coûts d'infrastructure et d'exploitation il lui a fallu augmenter et fidéliser sa clientèle et pour cela se présenter comme un moyen de déplacement fiable et sûr. Les préoccupations de sécurité ferroviaire des débuts visaient surtout à éviter des situations dangereuses propres à la circulation des trains. A partir d'une approche pratique, puis démonstrative jusqu'à une approche système globale, la notion de sécurité s'est donc, en 150 ans, formée, enrichie et adaptée pour devenir une véritable culture corporative. La réduction des risques était et est toujours fondée sur le principe de la démonstration dont une des particularités est de réduire à zéro la part laissée à l'improvisation. Mr JANDOT, ancien ingénieur à la SNCF, introduisait son cours sur l'électronique de sécurité ainsi : "Depuis plus de cent ans qu'elles existent les installations de sécurité des chemins de fer n'ont cessé de se développer et de se perfectionner. Elles peuvent être citées parmi les installations qui donnent la meilleure idée de ce que peut être la sécurité : elles ne sont pas soumises ou pratiquement pas aux risques d'erreur qui caractérisent l'intervention humaine. On a pu dire, depuis plusieurs dizaines d'années déjà, que si un singe pénétrait dans un poste d'aiguillage moderne et s'il actionnait les commandes au hasard, il ne provoquerait aucune catastrophe.". Ces quelques mots illustrent surtout le fait que le principe de l'approche démonstrative tel qu'il est admis par le ferroviaire n'est vrai que dans un environnement parfaitement connu et conçu pour répondre à des sollicitations identifiées ; cela est le cas d'une installation purement technologique. Le caractère guidé du chemin de fer autorise peu la créativité dans le comportement et toute situation dangereuse doit par conséquent être appréhendée avant son occurrence. Cependant des systèmes de transport autres comme les transports maritime, aérien et routier et même le tramway sont soumis à des environnements moins maîtrisables et font par conséquent appel à cette capacité des intervenants humains à réagir de manière créative. La notion de création n'implique pas l'improvisation. Elle ne doit pas être considérée comme l'expression d'un comportement chaotique ou erratique mais plutôt comme la capacité à créer de nouveaux comportements face à des situations nouvelles. Dans ce cas le niveau de sécurité relève autant de la confiance que l'on peut avoir dans la technologie que dans la compétence et la connaissance que l'intervenant humain peut avoir du comportement du système.

Le paramètre humain a été le premier paramètre considéré dans la sécurité des systèmes. Ainsi, sur les premiers réseaux ferrés français, le poste de conduite des locomotives n'était pas abrité car les concepteurs pensaient que le confort nuisait à la vigilance des conducteurs. Cette anecdote historique illustre le fait que pour les concepteurs d'équipements, la gestion des risques a pour objectif de réduire l'incidence des erreurs humaines et ainsi de minimiser le risque résiduel des défauts d'origine extérieure aux équipements liés à la sécurité.

La sécurité est fondée sur une identification et une couverture des cas critiques d'erreur ou de défaillance. Ceux-ci sont identifiés à partir de l'analyse de situations rencontrées; les règles de l'art pour la construction et l'exploitation sont ensuite définies à partir de solutions techniques dont l'expérience a démontré qu'elles présentaient des résultats satisfaisants. Ainsi, de manière générale, il est admis que la sécurité d'un système de transport repose sur une stratégie de conception et de réalisation dont l'objectif est de lutter contre l'erreur et la défaillance, et d'une politique de formation dont l'objectif est de conditionner le comportement des opérateurs humains.

Pour les concepteurs, la gestion des risques a surtout pour objectif de réduire l'incidence des défaillances intrinsèques et des erreurs humaines. Dans ce but, sont appliquées des méthodes

d'analyse et de gestion permettant de définir un environnement, d'évaluer les risques sur cet environnement et de déterminer un matériel et un domaine d'exploitation permettant de réduire ces risques à un niveau acceptable. La tâche de l'exploitant consiste ensuite à conserver le système dans le domaine de fonctionnement spécifié, et à anticiper les situations dangereuses identifiées.

Le système est maintenu dans un état de stabilité. Tout changement se traduit par une instabilité qui implique une adaptation du système. Cette instabilité s'accroit d'autant plus que les facteurs temps ou les comportements humains corrigent les hypothèses sur lesquelles ont été fondées la conception et la réalisation. Ainsi assurer la sécurité d'un système sur les seules démonstrations techniques de la sécurité, reviendrait à occulter complètement les habitudes, l'expérience et la mentalité des intervenants humains. Il suffit de travailler au contact des agents, techniciens et ingénieurs de la SNCF ou de la RATP, pour comprendre que la sécurité est autant une affaire de responsabilité personnelle que de technique et que le niveau de sécurité atteint par ces réseaux n'est pas dû qu'à la conception des équipements. Cet avis peut paraître très subjectif, mais les accidents survenus sur les réseaux d'outre Manche, dont tous s'accordent à dire qu'ils étaient dus à une dilution des responsabilités et à la perte du savoir faire, en fournissent une bonne démonstration.

La nécessité d'une maîtrise du risque est depuis longtemps acquise. Une ingénierie du risque s'est développée autour de ce besoin et a produit des techniques et des méthodes d'analyse et de gestion adaptées. Le besoin de pouvoir qualifier des chaînes fonctionnelles ou organiques plus complexe, et le besoin de garantir le respect d'un certain engagement de sécurité dès la conception a conduit à quantifier la notion de risque, puis à développer les méthodologies de l'ingénierie du risque. Si les premières approches étaient surtout pratiques et visaient à couvrir des risques techniques particuliers, la notion de sécurité s'est rapidement élargie au-delà de ces besoins pour prendre en compte les risques globaux du système. Les techniques d'analyse et de conception ont alors été complétées par des méthodologies visant à s'assurer de la cohérence globale des solutions développées. Cette approche globale de la gestion des risques s'appuie sur un document unique de démonstration de la sécurité. Ce document unique permet de s'assurer que l'ensemble des critères techniques, environnementaux et humains ont été pris en compte mais surtout que toutes les interfaces et interactions ne remettent pas en cause la sécurité du système. La mise en commun de sous systèmes divers et de techniques diverses exigent souvent la présence d'experts pour compléter les analyses formelles réalisées.

On constate que malgré la richesse du domaine en outils d'analyse, l'essentiel des modélisations s'appuie pour l'expression des concepts sur une vision structuraliste et sur une démarche analytique dans sa compréhension des systèmes. Aujourd'hui, les causes d'accident trouvant moins leur origine dans la défaillance technique que dans la défaillance des organisations humaines, les études de sécurité exigent des approches différentes. Le domaine s'enrichie d'approches plus large comme les approches cognitives, ou systémiques. Par opposition aux méthodes analytiques qui abordent toujours le système par ses organes ou ses flux, les méthodes systémiques cherchent à appréhender le système par son comportement et ses objectifs. Les principales approches systémiques proposées à ce jour tentent d'identifier les grands concepts permettant d'évaluer les critères représentatifs du comportement et établissent un nouvel espace sur lequel elles tendent de représenter le système. Malgré les apports certains que ces méthodes fournissent dans la connaissance des signaux annonciateurs des situations de danger, celles-ci reviennent toujours vers une description structurelle dans la représentation des systèmes.

Face à la complexification des systèmes, aux contraintes d'interopérabilité et au besoin de performances toujours plus élevées, il devient nécessaire de pouvoir établir des modèles compréhensibles et utilisables par les différents type d'intervenants, présentant le même caractère de décidabilité que les méthodes actuelles et offrant l'ouverture nécessaire pour la prise en compte de paramètres humains. Si les approches systémiques sont les seules qui permettent d'appréhender

un système dans sa globalité, les limites qu'elles rencontrent dans la représentation des systèmes doivent être dépassées. Le travail de recherche mené dans le cadre de cette thèse a été de déterminer les concepts nécessaires à une approche systémique complète depuis la conceptualisation du système jusqu'au modèle de calcul.

Après une définition des grands concepts de l'ingénierie du risque, le premier chapitre présentera largement les fondamentaux qui régissent les analyses de sécurité, en particulier les principes servant à déterminer les objectifs de performance de sécurité d'un système sous la forme d'un couple *gravité-occurrence*. Les raisonnements socio-économiques et les outils formels d'analyse et de calcul seront détaillés avant que ne soient abordées les méthodologies structurant les approches système. La fin de ce chapitre sera consacrée aux approches cognitives et systémiques aujourd'hui utilisées dans la maîtrise des risques.

Le second chapitre expose les objectifs qui ont été fixés à la démarche de recherche et les contraintes que doit respecter toute conceptualisation. En particulier un exposé des différences entre une démarche analytique et une démarche systémique permettra de comprendre les choix effectués par la suite.

Dans le troisième chapitre seront abordés les concepts permettant de proposer une modélisation systémique complète, en particulier le paradigme espaces-processus fondateur de l'approche proposée dans ce mémoire. Ce paradigme postule que tout système peut se définir comme un projet d'action c'est-à-dire une combinaison espaces-processus, les espace contenant toutes les conditions et moyens nécessaires à l'achèvement du processus. En premier lieu sera expliqué le modèle des espaces, modèle de la perception par la propriété permettant le couplage au langage qui est un des éléments essentiel dans l'utilisation de cette approche. Ensuite, les principes de la dynamique instanciation et transformation permettront de comprendre la structure de l'espace des processus.

Dans le quatrième chapitre seront définis tous les éléments sur lequel est fondé le modèle de représentation. En premier lieu, sera établi une notation de la propriété permettant de l'appréhender par une variable, par son domaine de définition et surtout par sa signification comme élément du langage. Le chapitre montrera qu'il est possible de définir n'importe quel comportement comme la somme d'expressions rationnelles de propriétés sur un espace général. Une forme algébrique des ces expression rationnelles sera ensuite proposée. A partir de cette forme algébrique le mémoire montrera comment leur manipulation permet de décrire toute les formes de relations, en particulier dans la chronologie des comportements. Le mémoire s'attachera à montrer comment le choix du système d'écriture formel d'une propriété associant sémantique et valeurs des réalisations permet de ne pas perdre le couplage avec le langage lors de la transposition du comportement vers l'expression rationnelle.

Aujourd'hui les différentes approches mettent l'acteur humain et l'organisation au centre des problèmes de gestion des risques, le cinquième chapitre présentera au lecteur, en complément du modèle représentation, un modèle de système général fondé sur la collaboration d'un système opérant, d'un système de connaissance et d'un système décisionnel fournissent une vision macroscopique nécessaire à l'appréhension de la complexité qui caractérise les systèmes à forte composante humaine. Il sera montré comment ce modèle général est utilisé dans une approche espaces-processus et en particulier comment l'organisation des différents acteurs du comportement du système se traduit dans les relations intervenant au niveau des propriétés

Le sixième chapitre abordera brièvement l'utilisation de l'approche modélisatrice *espaces – processus* dans une démarche d'analyse des risques. Il sera montré comment le fort couplage au langage par les unités sémantiques permet de conduire des analyses d'expert sur le modèle et surtout comment le transfert vers un espace probabilisé autorise l'utilisation les outils formels de quantification des probabilités d'occurrence d'événements ou de situations.

Le dernier chapitre présentera les conclusions du travail de recherche exposé et les perspectives de recherches complémentaires ouvertes par ces premiers résultats, en particulier dans l'exploitation des unités sémantiques dans l'exploitation du modèle ou dans l'ananlyse de schéma syntaxiques à travers de bases de connaissances.

L'INGENIERIE DU RISQUE ET LES SCIENCES DU DANGER

INTRODUCTION

Dans la littérature comme dans la vie courante sont employés fréquemment les termes de risque, danger, menace, accident… Aucun de ces termes ne recouvre pourtant les mêmes concepts ou les mêmes situations. Leur utilisation est très souvent induite par l'appréciation des dommages qui découlent de la situation et par la connaissance de l'événement qui l'a déclenchée. Par exemple, pour la circulation automobile, le danger est souvent rattaché aux conséquences d'un accident éventuel, alors que pour le terrorisme, le danger est lié à une menace identifiée, quelles que soient les conséquences des actions, celles-ci étant par définition létales. L'utilisation d'un terme ou d'un autre est souvent associée à la perception qu'à un interlocuteur des dommages connus ou supposés résultant d'un événement ou d'une situation et de leur potentialité. La confusion qui peut découler de leur interprétation vient de ce qu'ils sont porteurs d'une information complexe qui va être distordue par les échelles de valeurs du locuteur et par l'expression de son incertitude face à l'événement ou face aux conséquences. Ainsi l'amalgame de ces termes dégagés de leur contexte peut aboutir à des confusions. Il est donc illusoire de chercher une définition suffisante et non subjective des termes de danger, de risque, etc.

Quelles que soient les interprétations que chacun attribue à ces termes, ils vont porter une information relative à une séquence événement – situation – conséquence. Se dégagent alors de façon claire et non ambigüe, les notions suivantes :

- Evénement : fait survenant ou pouvant survenir. Cet événement sera alors normal, opportun, redouté, indésirable…
- Situation : résultat d'une combinaison d'événements. La potentialité d'une situation est donc directement liée à la potentialité des événements. Une situation sera normale, dégradée, redoutée, indésirable…
- Conséquences : impact d'une situation sur le monde environnant: objets, humains, environnement…
- Gravité : pondération des conséquences dommageables d'une situation.
- Occurrence : probabilité qu'a une situation de survenir sur un horizon de temps déterminé.

Les notions d'événement, de situation et de conséquence sont des notions descriptives. Compte tenu du lien qui existe entre événements et situations, et, entre situations et conséquences, il serait tentant d'essayer de réduire encore les notions utilisées. Or, il n'est pas possible de décrire un système uniquement à partir des événements et des conséquences ou même des seules situations.

La notion de risque associe un événement qualifié de redouté avec la probabilité de le voir se produire, on parle de gravité et d'occurrence. Les notions de gravité et d'occurrence sont des notions qualificatives complètement indépendantes. La notion d'occurrence est fondée sur une mesure (probabilité, statistique ou estimation) ; la notion de gravité réfère à la graduation de l'ampleur des conséquences de l'événement par rapport à une échelle de référence. La qualification du risque est constituée à la fois d'un critère objectif quantifiable, l'occurrence, et d'un critère subjectif de valeur, la gravité des conséquences ; il est communément admis de dire que le risque se définit par le couple gravité – occurrence

Néanmoins ce simple produit n'est pas suffisant pour déterminer de façon absolue le risque. En effet, les échelles ainsi déterminées par cette double qualification ont souvent pour objectif de répartir les risques dans des catégories elle-même déterminées par rapport à un niveau de non acceptation des conséquences des événements. Par exemple, un mort dans un accident de train correspond à un niveau de non acceptabilité très élevé, alors qu'un mort dans son propre camp au cours d'une guerre correspond au contraire à un niveau de non acceptabilité faible. On comprend que la notion de risque ou de danger peut selon les époques, les milieux socioculturels ou socioéconomiques, les stratégies ou les individualités, être perçue différemment.

Les cinq notions abordées ici représentent les radicaux communs du langage des gens du risque. Les trois notions événement, situation et conséquences sont relatives à l'identification des risques, gravité et occurrence permettant de l'évaluer.

Toute démarche menée dans le sens de la sécurité va soit tendre à réduire la probabilité qu'un événement se produise, soit tendre à réduire les conséquences de son occurrence. Ainsi, toutes les approches, méthodologies qui vont être décrites par la suite vont chercher à fournir la connaissance des paramètres nécessaires à la prise d'une décision : faut-il prévenir ou faut-il protéger?

L'évaluation du risque acceptable

La norme MIL-STD-882 [MIL 2002] définit la sécurité d'un système comme "égale au degré de sécurité optimale compatible avec les contraintes d'efficacité opérationnelle, les coûts et les délais, et qui doit être obtenu par application systématique des principes de sécurité (conception et conduite) au cours des phases successives de la vie du système".

Cette phrase révèle toute la difficulté qu'il y a à évaluer le niveau de risque acceptable étant donné que cette évaluation résulte d'un compromis entre les connaissances à un instant donné et le contexte économique dans lequel opère le système. La détermination de ce niveau de risque acceptable est la pierre angulaire de tout programme de gestion des risques car il va définir le niveau de la qualité et la quantité des moyens à mettre en œuvre pendant tout le cycle de vie du système.

La détermination des objectifs de sécurité, en particulier leur quantification, est une étape capitale et souvent délicate des processus de gestion des risques. La démarche est souvent une combinaison d'acquis personnel, de sentiments, et d'un référentiel de connaissances normatives dont on suit les prescriptions sans forcément en connaître les raisons.

Etablissement d'un référentiel quantifié du risque acceptable

D'une manière générale la détermination de la gravité est fortement liée l'échelle d'évaluation utilisée. Une approche communément utilisée pour quantifier la gravité des conséquences d'un accident sur un système de transport est le recensement des vies humaines perdues. La valeur de gravité établie est donnée en "équivalent victimes". En comptant 1 une vie perdue, les personnes sérieusement blessées peuvent être comptées 0.1, et les personnes légèrement atteinte 0.01 équivalent victime. Cependant cette approche ne tient pas compte des dommages matériels ou même du coût d'incapacité des blessures.

Il existe différentes échelles de gravité pour l'accident corporel selon le type d'accident et le pays d'application, citons par exemple:

- Le barème dit du Docteur Rousseau, publié dans la revue *Le Concours Médical* en 1982, est un barème anatomo-fonctionnel encore utilisé par les assureurs en France pour l'évaluation médico-légale des handicaps résultants d'accidents de la route, le taux de 100% d'incapacité correspond à la mort.
- L'Injury Severity Score défini par *L'American Association for Automotive Medecine* pour lequel les lésions de faible gravité sont évaluées sur une échelle de 1à 5, les lésions intermédiaires de 5 à 9 et les lésions graves évoluant au dessus de 10.

Nous constatons que dans un système mettant en commun la vie humaine et des infrastructures coûteuses la gravité est souvent le résultat d'une combinaison du nombre de victimes et du coût des dommages matériels. La détermination de ces échelles implique de définir les unités qui permettent de quantifier les gravités (coûts, nombre de jours d'arrêt de travail, taux d'invalidité, etc…) et de prendre en compte de nombreux paramètres comme les conséquences pour l'environnement ou le public, les effets sur l'économie ou le marché de l'emploi, ou même le confort de la communauté.

Des échelles de gravité prenant en compte les conséquences humaines (atteinte ou ressenti) et matérielles et leurs effets dans le temps sont quelquefois déterminées. Citons par exemple:

- l'échelle EMS-98 [EMS 1998], définie par le Conseil de l'Europe à partir de l'échelle MSK (du nom des trois sismologues Medvedev, Sponheuer et Karik qui l'ont proposée en 1964). Cette échelle à cinq niveaux prend en considération le ressenti d'un tremblement de terre et les différents types de dégâts qu'il a pu occasionner.
- L'échelle internationale des événements nucléaires [INES 2001], définie après Tchernobyl qui propose une classification à sept niveaux, de l'incident à l'accident majeur. Les événements sont classifiés en fonction des rejets vers l'extérieur de produits radioactifs mais aussi des dégâts causés à l'installation et des moyens d'intervention mis en œuvre.
- L'échelle de gravité des accidents industriels élaborée par l'OCDE en 1994 pour l'application de la directive SEVESO établit un indice de gravité à partir de dix-huit paramètres permettant de déterminer six niveaux de gravité en fonction des conséquences humaines, environnementales et financières [ARIA 2006].

Il est aussi possible d'utiliser une approche économique optimisant le rapport entre l'utilité sociale du système et le coût direct ou indirect que la communauté aurait à supporter pour mettre en œuvre le système. L'utilité sociale d'un système est égale à la contribution de l'activité au revenu annuel moyen de l'individu. L'utilité d'un système de transport fait intervenir le coût direct supporté par le passager et le temps gagné par rapport à un système moins rapide.

Ces échelles déterminent un niveau de gravité auquel il est possible d'associer un seuil d'acceptabilité mais ne fournissent aucune indication sur les moyens à mettre en œuvre pour réduire le risque associé.

La détermination d'une combinaison de valeurs de gravité et d'occurrence reste problématique. S'il est possible de choisir une unité de référence dans la détermination des conséquences en se basant sur les coûts des dommages matériels, les coûts de reconstruction ou même sur les coûts des assurances pour évaluer les dommages humains, ces paramètres ne peuvent pas prendre en compte le facteur psychologique associé au risque que représente la crainte et l'aversion qu'a le public pour les accidents matériels en particulier lorsque le risque n'est pas pris volontairement. Un bon indicateur de cette réalité est le temps d'antenne accordé aux 350 morts dans le monde par catastrophe aérienne à comparer au temps d'antenne accordé aux 4500 morts par accident de la route sur le seul territoire français.

Différentes approches ont été menées pour déterminer des niveaux quantifiés de risques acceptables : par exemple les approches de Chauncey Starr [STARR 1969], de F.C. Farmer [LIEVENS 1976], de Kuhlmann [KULHMANN 1986], de Kafka [KAFAK 1999]. Nous allons voir que ces approches sont assez similaires dans la démarche et aboutissent toutes à l'élaboration d'un diagramme à deux dimensions sur lequel il est possible de représenter les zones de risques acceptables et les zones de risques inacceptables.

Starr [STARR 1969] a tenté d'établir une corrélation entre la probabilité d'accident mortel par heure d'exposition au risque et l'utilité sociale. L'heure d'exposition a été retenue comme la plus simple unité utilisable pour des activités de caractères très différents. En revanche, cette unité devient critiquable lorsqu'il s'agit d'évaluer la sécurité de moyens de transports pour un trajet donné ; le kilomètre parcouru ou le nombre de passagers transportés peuvent être alors plus pertinent.

En examinant les taux d'accidents mortels dans diverses industries d'extraction (carrières et mines), Starr est arrivé à la conclusion que le risque acceptable est sensiblement proportionnel

au cube de l'utilité sociale exprimée en Dollars. Cette hypothèse conduit au graphique de la Figure 1 sur lequel Starr a fait apparaître plusieurs activités volontaires ou imposées pour comparaison.

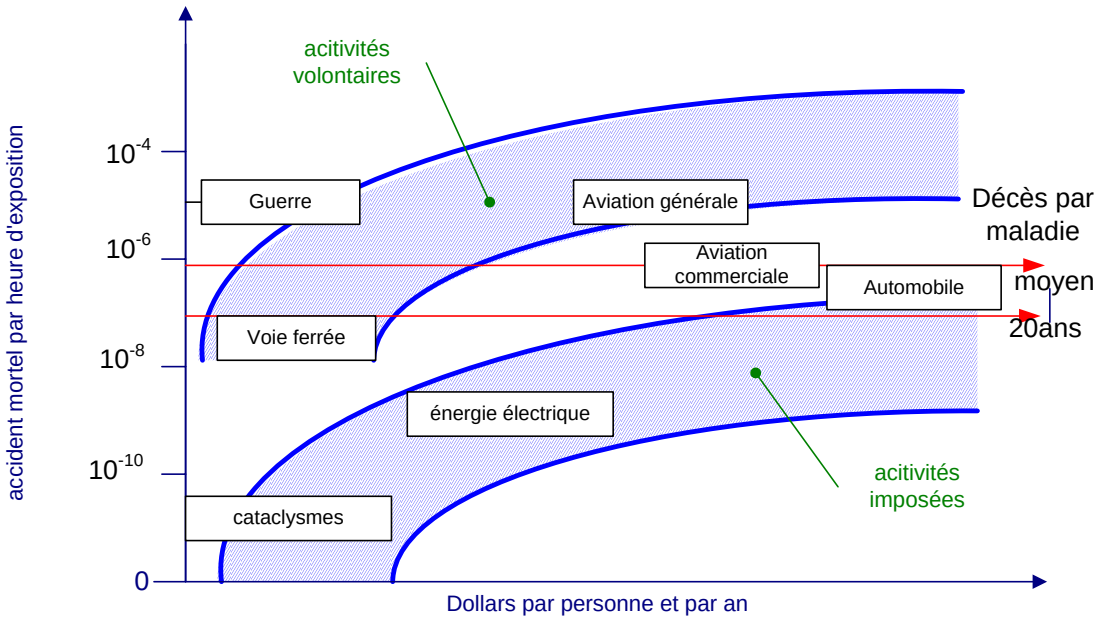


Figure 1 : Critère de Chauncey Starr [LIEVENS 1976]

Il apparaît immédiatement qu'il existe une différence de plusieurs ordres de grandeurs entre les niveaux de risques acceptables suivant qu'il s'agit :

- d'activités volontaires pour lesquelles l'individu utilise sa propre échelle de valeurs pour prendre ses décisions et juger ses expériences,
- d'activités imposées par la société pour lesquelles le compromis est entre les mains d'autorités organisatrices relativement éloignées des individus exposés au risque.

On constate que le risque de mort par maladie joue un rôle certain dans la détermination d'un critère d'acceptabilité pour les activités volontaires. Par contre, il n'est pas possible de faire une distinction entre les niveaux de risques des activités volontaires et des activités imposées. Aussi, Starr a-t-il définit une fonction de la conscience sociale de l'utilité en faisant intervenir en plus des deux premiers facteurs (probabilité de risque et coût de l'utilité sociale) le montant relatif des dépenses de publicité pour permettre l'acceptation du risque.

Un autre type d'approche a été utilisé sur l'idée que chaque évènement est caractérisé par sa probabilité et par son coût. Il existerait alors dans le plan probabilité – coût une délimitation entre une zone acceptable et une zone inacceptable. En représentation logarithmique une telle fonction fournirait une droite de pente négative décrivant une probabilité maximale admissible, fonction décroissante de la gravité (gravité exprimée ici par son coût). L'effet pervers de ce critère est qu'en décomposant un évènement redouté inacceptable en deux évènements distincts on peut le rendre acceptable. C. Lievens [LIEVENS 1976] regrette que cette manipulation purement formelle puisse apparaître comme un moyen de démonstration de la sécurité et propose : soit d'adopter un objectif global de sécurité, soit d'imposer une méthode de recherche des évènements excluant une possibilité de décomposition abusive.

Il est intéressant de noter qu'il n'existe pas de référence absolue permettant de fixer les objectifs de sécurité. En effet, et en particulier dans les transports, il est impossible de faire

admettre à un passager qu'il ne voyage pas dans une sécurité absolue mais avec une probabilité réduite d'avoir un accident.

Le principe de risque acceptable associé à la mortalité endogène a été développé par Kuhlmann dans son approche [KULHMANN 1986]. Kulhmann prend pour seuil de référence le taux de décès naturel c'est-à-dire non causé par la proximité ou l'utilisation de systèmes techniques, par des épidémies ou tout autre cause ne contribuant pas à la mortalité endogène. Kulhmann a aussi constaté que ce taux de mortalité endogène avait son minimum sur les populations âgées de 15 à 20 ans. La probabilité statistique de décès établie par individu et par année est de 2.10^{-4}. Kuhlmann a fixé comme objectif que tout système technologique doit être conçu pour ne pas contribuer à l'augmentation du risque de mortalité d'un individu et à proposé une échelle déterminant le niveau de risque acceptable inférieur au taux de mortalité endogène.

Nombre de victimes potentielles par accident	**Seuil acceptable par personne et par an**
1	10^{-5}
10	10^{-5}
100	10^{-5}
1000	10^{-6}
10 000	10^{-7}
100 000	10^{-8}
1 000 000	10^{-9}

Figure 2 : Critère de kulhmann [KULHMANN 1986]

Le tableau de Kulhmann définit un seuil de probabilité d'accident touchant une, dix, cent et ainsi jusqu'à un million de personnes. Les dernières valeurs peuvent paraître irréelles, si on se place simplement du côté du transport de voyageur, mais si on prend en compte l'aspect impact environnemental, ils correspondent alors à des événements de dimension catastrophique à l'échelle de Bopal ou Tchernobyl. Cette échelle a été déterminée pour des accidents ayant pour conséquence plus d'un décès et en prenant en compte l'aspect psychologique d'accidents faisant plus de 100 victimes. L'autre particularité est que cette échelle définit un niveau de risque subi par personne et par an. Kulhmann propose d'utiliser les valeurs de risque maximum tolérable suivantes pour un système technique :

- 10^{-5} décès par personne et par an,
- 10^{-4} incapacité permanente par personne et par an,
- 10^{-3} incapacité temporaire par personne et par an.

C'est-à-dire qu'un système transportant 1 000 000 de passagers par an ne devra pas provoquer plus de 10 décès, 100 incapacités permanentes et 1000 incapacités temporaires.

Kulhmann rapproche ces valeurs des statistiques d'accident fatal dans différentes industries au cours de l'année 1980.

Industrie	**Accident fatal par personne et par heure**
Mines	$3\ 10^{-7}$
Métiers de la route	$3\ 10^{-7}$
Construction	$2\ 10^{-7}$
Industries des métaux non ferreux	$1.5\ 10^{-7}$
Gaz et eau	$4\ 10^{-8}$

Industrie	Accident fatal par personne et par heure
Industrie sidérurgique	710^{-8}
Industrie du bois et pâtes à papier	$4\ 10^{-8}$
Agroalimentaire	$6\ 10^{-8}$
Industrie du livre	$5\ 10^{-8}$
Electronique, optique et mécanique de précision	$4\ 10^{-8}$
Chimie	$3\ 10^{-8}$
Commerce, finances et assurances	$5\ 10^{-8}$
Textiles et cuirs	$2\ 10^{-8}$
Services de santé	10^{-8}

Figure 3 : Statistiques d'accident fatal pour l'industrie en 1980 [KULHMANN 1986]

Autre exemple de démarche, Kafka [KAFKA 1999] a compilé les données de différentes sources pour établir une table des risques d'accident mortel par heure d'exposition au risque.

Région et type de transport	Information utilisée	Risque d'accident mortel par heure	Hypothèse de péréquation
Ferroviaire, Japon	1 mort pour $1.3\ 10^{12}$ passagers x kilomètres	$6.2\ 10^{-11}$	Vitesse moyenne 80km/h
Ferroviaire, Allemagne	0.5 accident pour 10^{6} trains de fret km, perte supérieure à 1500€		
Route, Japon	15 accidents mortels pour 10^{9} passagers x km	$4.5\ 10^{-7}$	Vitesse commerciale moyenne 30km/h
Aviation	6.7 décès potentiels par 10^{9} miles parcourus x passagers	$2.7\ 10^{-6}$	Vitesse moyenne passager 400 miles/h
Véhicules motorisés	Risque potentiel de décès de $8\ 10^{-5}$ par passager sur la base	$1.6\ 10^{-8}$	Vitesse moyenne 20 miles/h
Cancer (tous âges), Royaume Uni	Risque potentiel de décès : 1/350	$3.3\ 10^{-7}$	Exposition permanente (8760 heures dans l'année)
Route, Royaume Uni	Risque potentiel de décès : 1/11000	10^{-8}	
Mines de charbon	Risque potentiel de décès : 1/7000	$1.6\ 10^{-8}$	
Accidents domestiques	Risque potentiel de décès : 10-4 par an	$1.1\ 10^{-8}$	
Accidents de travail, Royaume Uni	Risque potentiel de décès : 1/70000	$1.6\ 10^{-9}$	
Foudroiement, Royaume Uni	Risque potentiel de décès 1/ 10 000 000	$1.1\ 10^{-11}$	

Figure 4 : Données de risques de KAFKA [KAFKA 1999]

Détermination des seuils d'acceptabilité

La détermination des critères d'acceptabilité obéit à des approches qui peuvent paraître subjectives. En effet, en dehors de l'aviation pour laquelle les règles fixent la valeur maximale de risque acceptable d'accident (la probabilité d'accident ne doit jamais être supérieure à 10^{-9} par heure de vol pour les passagers), de nombreux systèmes de transport, et en particulier de transport ferroviaire, sont conçus par application de grands principes :

- Principe ALARP (As Low As Reasonably Praticable) pratiqué au Royaume Uni : "tout risque doit être réduit autant qu'il est raisonnablement admissible, ou à un niveau aussi bas qu'il est raisonnablement possible de le faire",
- Principe GAME (Globalement Au Moins Equivalent) pratiqué en France : "la modification d'un système existant, la conception ou la mise en œuvre d'un nouveau système doivent être réalisées de telle façon que le niveau global de sécurité de l'installation après modification est au moins équivalent au niveau actuel de sécurité ou au moins équivalent au niveau de sécurité d'une installation de référence produisant les mêmes services ou fonctionnalités",
- Principe MEM (Mortalité Endogène Minimale) pratiqué en Allemagne : "tout risque dû à un nouveau système de transport ne doit pas significativement augmenter le valeur du risque de mortalité endogène auquel un individu qui l'utilise est normalement exposé".

Nous ne décrirons pas ici en détail ces principes qui seront repris dans le paragraphe sur l'évaluation de l'acceptabilité du risque, cependant il faut noter les différences fondamentales suivantes:

- le principe MEM considère le risque individuel, alors que la démarche ALARP prend en compte le risque collectif appliqué à la société dans son ensemble. Le principe GAME est applicable aussi bien au risque individuel que collectif.
- Les principes MEM et GAME offrent un seuil de risque tolérable à ne jamais franchir. Par contre, le principe ALARP fonctionne avec deux limites : la limite haute de risque à ne jamais franchir, et, une limite basse en dessous de laquelle le risque est toléré. La zone intermédiaire entre les deux limites est la zone dite ALARP dans laquelle le risque est considéré acceptable s'il est démontré que tout ce qui pouvait raisonnablement être réalisé pour le réduire a été mis en œuvre. Ce dernier principe implique que l'acceptation d'un risque relève d'un compromis économique entre le coût de la réduction de ce risque et le coût induit par l'accident potentiel.

Enfin, la notion d'intégrité de la sécurité d'un système, SIL (System Integrity Level). Cette notion caractérise l'aptitude de celui-ci à remplir les fonctions de sécurité requises. Plus le niveau de sécurité requis est élevé moins il est à craindre que le système ne remplisse pas ses fonctions de sécurité. La notion de SIL s'applique essentiellement aux systèmes techniques et définit le risque maximum tolérable par heure de fonctionnement. La notion d'intégrité de la sécurité se matérialise par une échelle comportant quatre niveaux discrets appelés niveaux de SIL. Les SIL sont un moyen utilisé pour faire correspondre les approches qualitatives non quantifiables. L'intégrité comprend deux conditions auxquelles il est nécessaire de satisfaire pour atteindre le niveau requis:

- l'intégrité vis-à-vis des défaillances systématiques
- l'intégrité vis-à-vis des défaillances aléatoires.

L'intégrité vis-à-vis des défaillances systématiques représente la partie non quantifiable de l'intégrité car elle correspond aux erreurs dues à des erreurs humaines pendant les différentes phases du cycle de vie du système. Parmi ces erreurs, on peut citer : les erreurs de spécification, de

conception, de fabrication ou d'installation, mais aussi, les erreurs d'exploitation, de maintenance ou de modifications. La réduction des risques dus à ces erreurs repose sur l'ensemble des méthodes de conception et réalisation soutenues par des dispositions de gestion de la qualité et de la sécurité déjà abordées dans le chapitre précédent. L'intégrité vis-à-vis des défaillances aléatoires est la partie de l'intégrité de la sécurité relative en particulier aux défaillances matérielles résultant de la fiabilité des composants. L'évaluation est menée au moyen des calculs de probabilité effectués à partir des données connues des modes et des taux de défaillance des composants. Dans le cas particulier des composants conçus en sécurité intrinsèque, le taux de défaillance dangereuse est ramené à zéro bien que le risque résiduel d'une telle défaillance continue d'exister. A chaque niveau de SIL correspond une obligation d'organisation, de méthodes de conception, de réalisation et d'essais, des procédures de fabrication particulières, etc.

Le principe du SIL se retrouve dans les normes EN 50-129 [EN50129], EN 61508 [EN61508] et DEF STAN 00-56 [DEF 1996]. Si ces normes définissent 4 niveaux de SIL, elles ne leur attribuent par les mêmes objectifs quantifiés.

SIL	EN 50129 et EN 61508	DEF STAN 00-56
4	10^{-9}/h < < 10^{-8}/h	Lointain ≈ 10^{-8}/h
3	10^{-8} /h < < 10^{-7}/h	Occasionnel ≈ 10^{-7}/h
2	10^{-7} /h < < 10^{-6}/h	Probable ≈10^{-6}/h
1	10^{-6}/h < < 10^{-5}/h	Fréquent ≈10^{-5}/h

Figure 5 : Définition des niveaux de SIL

Le niveau de SIL0 correspond à une relative absence de risque.

Les valeurs données concernent l'occurrence d'une défaillance dangereuse d'un système technique soumis à une forte sollicitation. Les probabilités associées d'accident ne sont pas nécessairement identiques; en effet, et fort heureusement, toute défaillance technique ne conduit pas à un handicap physique ou au décès de l'usager.

La transformation du risque acceptable en objectif de sécurité

Avant de concevoir et d'organiser le fonctionnement d'un système il est nécessaire de transformer les niveaux de risques acceptables en objectifs de sécurité quantifiés. La démarche consiste à déterminer un ensemble de couples (gravité, occurrence) définissant la probabilité de sinistre tolérable pour une échelle de sinistres donnée.

Pour comprendre cette démarche de transformation l'exemple est la meilleure approche.

Nous allons mener une démarche heuristique qui va consister à déterminer des objectifs de sécurité afin que le système envisagé n'accroisse pas le risque individuel qu'encourt un passager même s'il n'utilise pas le système ; cela consiste à refuser d'augmenter de façon significative le risque individuel au-delà du taux de mortalité endogène.

Avant de déterminer les probabilités d'occurrence acceptables, il faut fixer l'échelle des gravités ; c'est-à-dire passer de la notion de mortalité d'un individu à des notions de préjudice

(sinistre n'entraînant pas la mort) et de catastrophe (sinistre entraînant plusieurs morts). Il devient nécessaire d'utiliser une unité en équivalent-victimes. En fixant la valeur 1 équivalent-victime pour un décès, il est possible de fixer une valeur pour un blessé grave (incapacité permanente) et une valeur pour un blessé léger (incapacité temporaire). Par exemple, en continuant d'utiliser l'approche de Kulhman nous pouvons établir la valeur 0,1 pour le blessé grave et 0,01 pour le blessé léger. Il faut noter toutefois que ces ratios, établis ici de façon simpliste, font l'objet de calculs intégrant les aspects économiques du secours, des soins et des jours d'invalidité (coût de l'arrêt de travail ou de la pension). Ce qui, si on ramène la notion de gravité sur un seul critère financier, peut éventuellement conduire à ce qu'un équivalent-victime pour un blessé grave est une valeur supérieure à 1.

Pour définir la limite haute de la gravité, nous allons choisir un réseau tramway transportant au maximum 60000 personnes par jour ; nous considérerons alors les sinistres avec 10 et 100 équivalents-victimes ce qui représente une catastrophe majeure pour ce type de système. Nous venons d'établir une échelle de log 0,01 à log100, de cinq catégories de gravité.

Pour déterminer les occurrences d'accident par catégorie, nous allons dans cet exemple utiliser les données de risque admissible pour les systèmes défini par Kulhmann [KULHMANN 1986] comme objectif global. Ce choix est purement arbitraire et n'a été fait que pour servir la démonstration ; un opérateur ou une autorité organisatrice des transports commencerait par utiliser des données statistiques à jour.

En fixant cette valeur nous établissons alors que la somme de toutes les probabilités de sinistre pour le système considéré ne doit pas dépasser la somme des seuils acceptables d'accident par personne et par an tel qu'il sont définis dans le tableau de la Figure 2, pour les catégories 1, 10 et 100 victimes. Cette somme correspond à un seuil acceptable d'accident par personne de 10^{-3} (0,00001 pour un accident d'une victime + 0,00009 pour un accident de 10 victimes + 0,0009 pour un accident de 100 victimes).

Pour déterminer la probabilité limite d'accident sur le système de transport, nous allons déterminer la courbe gravité – occurrence dont la probabilité totale de sinistre est inférieure à 10^{-3} c'est-à-dire dont l'intégrale sur [0.01, 100] a pour valeur 10^{-3}. En posant, que nous cherchons à établir une fonction continue et monotone, cette courbe est une progression géométrique sur le nombre d'équivalent - victimes du type de la forme $f(n) = kn^{\alpha}$ avec n le nombre d'équivalent-victimes et k nombre d'équivalent victimes pour la catégorie « blessés légers » et α le ratio du nombre d'équivalents victimes entre deux catégories.

C'est-à-dire qu'en considérant les catégories de gravité, il est possible d'écrire que

$$\sum_{n=0,01}^{n=100} (\log k + \alpha \log n) = 10^{-3}$$

Ce qui permet de déterminer les constantes a = -0,75 et k = 0.4217.

Catégorie de gravité en nombre d'équivalents victimes	Nombre d'accident maximum par catégorie	Probabilité d'accident de la catégorie par personne et par an pour 21900000 voyageurs transportés
0,01	13,335	$0,61\ 10^{-6}$
0,1	2,371	$0,11\ 10^{-7}$
1	0,422	$0,19\ 10^{-9}$
10	0,075	$0,34\ 10^{-10}$
100	0,0131	$0,59\ 10^{-11}$

Figure 6 : Exemple de détermination de seuil de gravité – occurrence

Le tableau ainsi obtenue (Figure 6) fournit un objectif de sécurité sous forme d'un seuil haut de probabilité d'accident par type de sinistre et par an. On remarquera que les objectifs déterminés sont acceptables en ce sens que s'il les respecte, le système n'augmente pas de façon significative le taux de mortalité endogène d'un usager.

La démarche choisie dans cet exemple a permis de fixer une limite haute du seuil de potentialité d'un accident sur le système de transport en fonction de ses conséquences. C'est-à-dire qu'un risque supérieur à ce seuil n'est pas toléré et que tous les moyens doivent être mis en œuvre pour que la potentialité d'accident ne dépasse pas ce seuil. Néanmoins, le même effort n'est économiquement pas réalisable pour réduire un risque dont la potentialité est proche du seuil que pour réduire un risque significativement inférieur. En effet, il existe en dessous de ce seuil une zone dans laquelle la potentialité d'accident est tellement faible qu'elle devient non significative et entre ces deux extrêmes une zone ou le risque doit être évalué pour déterminer s'il est tolérable et dans quelles conditions. Tolérable ne signifie pas que le risque est accepté mais qu'il est toléré face au bénéfice attendu de l'utilisation du système ou de la fonctionnalité, ou, qu'il est toléré parce que le coût des conséquences reste inférieur aux moyens à mettre en œuvre pour le réduire. Il est par conséquent nécessaire de déterminer une limite basse en dessous de laquelle le risque est accepté. La zone comprise entre ces deux limites est appelée zone ALARP. Cette démarche est une démarche purement économique; en effet, une valeur de risque inférieure à la limite basse ALARP ne signifie pas que le risque est faible, mais que la potentialité des dépenses à réaliser pour faire face aux conséquences de l'accident sont non significatives par rapport à la dépense systématiquement réalisée pour réduire le risque.

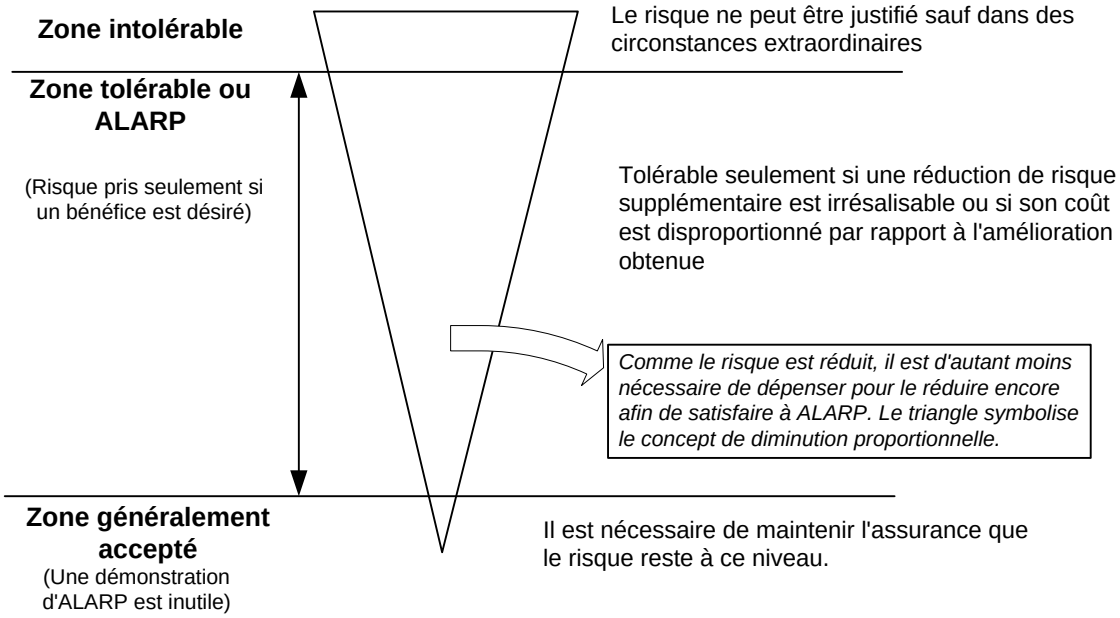


Figure 7 : zone ALARP [EN 61508]

Il est évident que la démarche de définition des objectifs quantifiés de sécurité d'un système de transport n'est pas une opération triviale. En effet, les opérateurs des systèmes de transport, les industriels ou les autorités organisatrices définissant les objectifs de sécurité d'un système sont confrontés à :

- La préoccupation individuelle : quelle valeur de risque ajouté par heure d'utilisation du système l'usager tolère-t-il d'ajouter à son propre budget risque (approche MEM).
- La préoccupation sociale : quel niveau de risque collectif la société veut-elle bien admettre en regard des services attendus du système. Le niveau de risque défini peut concerner le système global, comme certaines fonctionnalités offrant certaines performances (par exemple, fonction du nombre de passager transporté au même moment ou de la vitesse commerciale offerte). Cette démarche correspond donc à un compromis économique entre l'investissement réalisé pour réduire les niveaux de risques et le retour sur investissement attendu sur la solution. (approche ALARP).
- La préoccupation pratique : il est nécessaire de définir un objectif de risque maximal tolérable par unité (kilomètre parcouru, heure d'exploitation, véhicule en circulation) de façon à fournir aux industriels et aux opérateurs des spécifications réalisables, vérifiables et réalistes. l'objectif est-il cohérent avec la technologie et les crédits disponibles.
- Enfin, la préoccupation de progrès : tout nouveau système ou toute nouvelle solution ne doit pas offrir un niveau de sécurité inférieur aux anciens systèmes (principe GAME).

On s'aperçoit donc que l'exercice qui consiste à fixer des valeurs de risques déterminées en fonctions de conséquences auxquelles sont allouées des fréquences tolérables est un problème complexe. Les objectifs de sécurité sont à la fois qualitatifs et quantitatifs. Au vu de ce qui précède, il est facile d'imaginer les difficultés à définir et à allouer un niveau de risque acceptable quantifié à chaque type d'évènement. C'est une des raisons pour lesquelles les objectifs de sécurité sont déterminés « dans l'isolement des bureaux et consignés dans des documents à faible diffusion » (sic) [LIEVENS 1976].

Comme il est peu aisé de déterminer des objectifs de sécurité par catégorie, la démarche de classification s'appuie souvent sur des textes normatifs dans la démarche de classification. Ces textes fournissent alors des critères pour guider l'analyse tout en conservant un objectif global admis par l'ensemble des autorités du domaine. Pour ces diverses raisons, le recours aux normes apparaît comme la méthode de détermination des objectifs de sécurité la plus évidente, juridiquement la moins risquée et la moins polémique.

La classification des risques

Parler de la classification du risque avant d'aborder le sujet de l'identification du risque correspond à cette même logique qui est de déterminer les objectifs des études de sécurité avant de les mener. Ici le risque n'est pas considéré par l'événement qui conduit à l'accident mais toujours par la gravité de la conséquence.

De même que la détermination des objectifs de sécurité qui représente un seuil d'acceptation, la pondération du risque est faite à partir d'hypothèses sur la fréquence et la gravité des conséquences des situations dangereuses. Dans le cas où des valeurs sont utilisées celle-ci ne doivent pas être lues ou utilisées comme des seuils absolus délimitant des zones bien séparées mais comme des valeurs définissant des critères limites des zones.

La classification des risques permet par la distribution de ceux-ci en catégories de qualifier l'effort qui doit être produit pour éviter l'occurrence d'une situation aboutissant à la catégorie de conséquence correspondante.

Les deux tableaux ci-dessous, extraits de la norme EN 50126, décrivent les critères qualitatifs de fréquence et de gravité communément utilisés dans le ferroviaire.

Catégorie	*Description*
Fréquente	Susceptible de se produire fréquemment. La situation dangereuse est continuellement présente.
Probable	Peut survenir à plusieurs reprises. On peut s'attendre à ce que la situation dangereuse survienne souvent.
Occasionnelle	Susceptible de survenir à plusieurs reprises. On peut s'attendre à ce que la situation dangereuse survienne à plusieurs reprises.
Rare	Susceptible de survenir à un moment donné du cycle de vie du système. On peut raisonnablement s'attendre à ce que la situation dangereuse se produise.
Improbable	Peu susceptible de se produire mais possible. On peut supposer que la situation dangereuse peut exceptionnellement se produire.
Invraisemblable	Extrêmement improbable. On peut supposer que la situation dangereuse ne se produira pas.

Figure 8 : Tableau de fréquence des situations dangereuses [EN 50126]

Niveau de gravité	*Conséquence pour les personnes ou l'environnement*
Catastrophique	Des morts et/ou plusieurs blessés graves et/ou des dommages majeurs pour l'environnement.
Critique	Un mort et/ou une personne grièvement blessée et/ou des dommages graves pour l'environnement.
Marginal	Blessures légères et/ou menace grave pour l'environnement.
Insignifiant	Eventuellement une personne légèrement blessée.

Figure 9 : Tableau des catégories de gravité des situations dangereuses [EN 50126]

Ces critères permettent de produire une matrice bidimensionnelle « Occurrence-Gravité », telle que dans l'exemple ci-dessous, permettant d'attribuer un niveau de risque correspondant à un niveau d'acceptabilité.

Fréquence d'une situation dangereuse	Niveau de gravité des conséquences d'une situation dangereuse			
	Insignifiant	Marginal	Critique	Catastrophique
Fréquente	Indésirable	Inacceptable	Inacceptable	Inacceptable
Probable	Acceptable	Indésirable	Inacceptable	Inacceptable
Occasionnelle	Acceptable	Indésirable	Indésirable	Inacceptable
Rare	Négligeable	Acceptable	Indésirable	Indésirable
Improbable	Négligeable	Négligeable	Acceptable	Acceptable
Invraisemblable	Négligeable	Négligeable	Négligeable	Négligeable

Figure 10 : Matrice type occurrence - gravité suivant [EN 50126]

- Inacceptable : Doit être éliminé.
- Indésirable : Le risque n'est acceptable que lorsque la réduction de celui-ci est impossible ; dans ce cas l'accord de l'exploitant ou des autorités de tutelle du réseau est impératif.
- Acceptable : Le risque est acceptable moyennant un contrôle approprié et l'accord de l'exploitant ou de l'autorité de tutelle.
- Négligeable : Acceptable sans condition.

Ces critères ne sont fournis dans les normes qu'à titre indicatif; pour limiter les critères de décision il arrive souvent que les catégories d'occurrences soient ramenées à fréquent, occasionnel, rare, extrêmement improbable et les critères de risques résultants à acceptable et inacceptable. Cette classification permet souvent d'affecter directement les niveaux de SIL aux fonctions ou composants techniques qui réalisent tout ou partie de ces fonctions. Il est coutumier de classer les fonctions ou composants en trois catégories :

- SIL4 et SIL3 : Critique pour la sécurité ou de sécurité : si les risques sont inacceptables ou indésirables,
- SIL 2 et SIL1 : Non critique pour la sécurité si les risques sont tolérables,
- SIL0 : N'engageant pas la sécurité si le risque est négligeable.

L'identification des risques

L'objectif des analyses de sécurité

Nous avons vu dans les paragraphes précédents que la détermination des objectifs de sécurité consiste à déterminer des seuils tolérable ou non de probabilité d'accident en fonction de la gravité de ses conséquences. Ces niveaux ne caractérisent pas un système mais fixent la hauteur de l'effort consenti pour éviter que puisse se produire un accident. Il reste maintenant à identifier les accidents que l'on veut éviter : c'est là la démarche d'identification du risque.

Cette démarche est le processus qui permet de trouver et caractériser les situations ou les conditions comportant en elle-même un potentiel d'accident. Ces situations ou conditions sont appelées les risques ou les dangers, la démarche *analyse des risques* ou *analyse des dangers*.

L'analyse des risques est une étape qui permet :

- d'identifier la nature des dangers,
- de définir la matérialisation de ces dangers,
- d'identifier les différentes circonstances ou menaces susceptibles de faire se matérialiser le danger,
- d'identifier les faits ou événements pouvant être à l'origine des situations : événements redoutés,
- d'identifier les conséquences possibles suite à la survenance de ces événements.

Les facteurs influençant la sécurité

Dans l'approche système, la sécurité d'un système dépend de trois éléments :

- Les conditions système relatives aux défaillances internes au système lors de chaque phase de son cycle de vie.
- Les conditions d'exploitation relatives aux défaillances survenant au cours de l'exploitation du système.
- Les conditions de maintenance relatives aux défaillances survenant au cours des opérations de maintenance.

Pour réaliser des systèmes sûrs, il est nécessaire d'identifier les facteurs d'influence de la sécurité du système, d'en évaluer les effets et d'en maîtriser les causes tout au long du cycle de vie du système. Il y a trois catégories de facteurs d'influence:

Les facteurs génériques : facteurs d'influence qui se retrouvent sur toutes les applications industrielles. S'y retrouvent les caractéristiques techniques des équipements et composant y compris leurs modes de défaillances, les conditions d'environnement, les perturbations (électromagnétiques, climatiques…), les évènements naturels, le vandalisme, quoique ce dernier ne soit pas toujours convenablement pris en compte dans les études de sécurité.

Les facteurs spécifiques du domaine d'activité : Il s'agit des facteurs spécifiques à la nature des installations et à leur exploitation. Pour l'exploitation du système il s'agit des tâches que le système doit accomplir, des conditions dans lesquelles elles doivent être accomplies, de la coexistence avec d'autres systèmes techniques ou une infrastructure déjà existante dans un contexte opérationnel, des exigences liées à la vie du système, y compris sa durée de vie prévue, la

densité du service, ainsi que les exigences de coût, et enfin, les différentes catégories de défaillances et leur effets sur le type de système en fonctionnement normal, dégradé ou perturbé.

Les facteurs du comportement humain : une analyse des facteurs humains du point de vue de leurs effets sur la sécurité d'un système fait intrinsèquement partie de l'approche système. Les applications de transport impliquent en général une grande variété de groupes humains, depuis les passagers, le personnel d'exploitation et de maintenance, et le personnel chargé de la réalisation des systèmes jusqu'aux personnes concernées par l'exploitation telle que par exemple les automobilistes aux passages à niveau. Chacun est susceptible face à une situation identique de réagir de manière différente. Il est alors clair que le facteur humain à un impact potentiel important sur la sécurité du système.

L'organigramme page suivante tiré de la norme ferroviaire EN50-126 [EN50126], "spécification pour la démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité" résume sous forme d'une décomposition analytique ces différents facteurs d'influence pour le domaine ferroviaire.

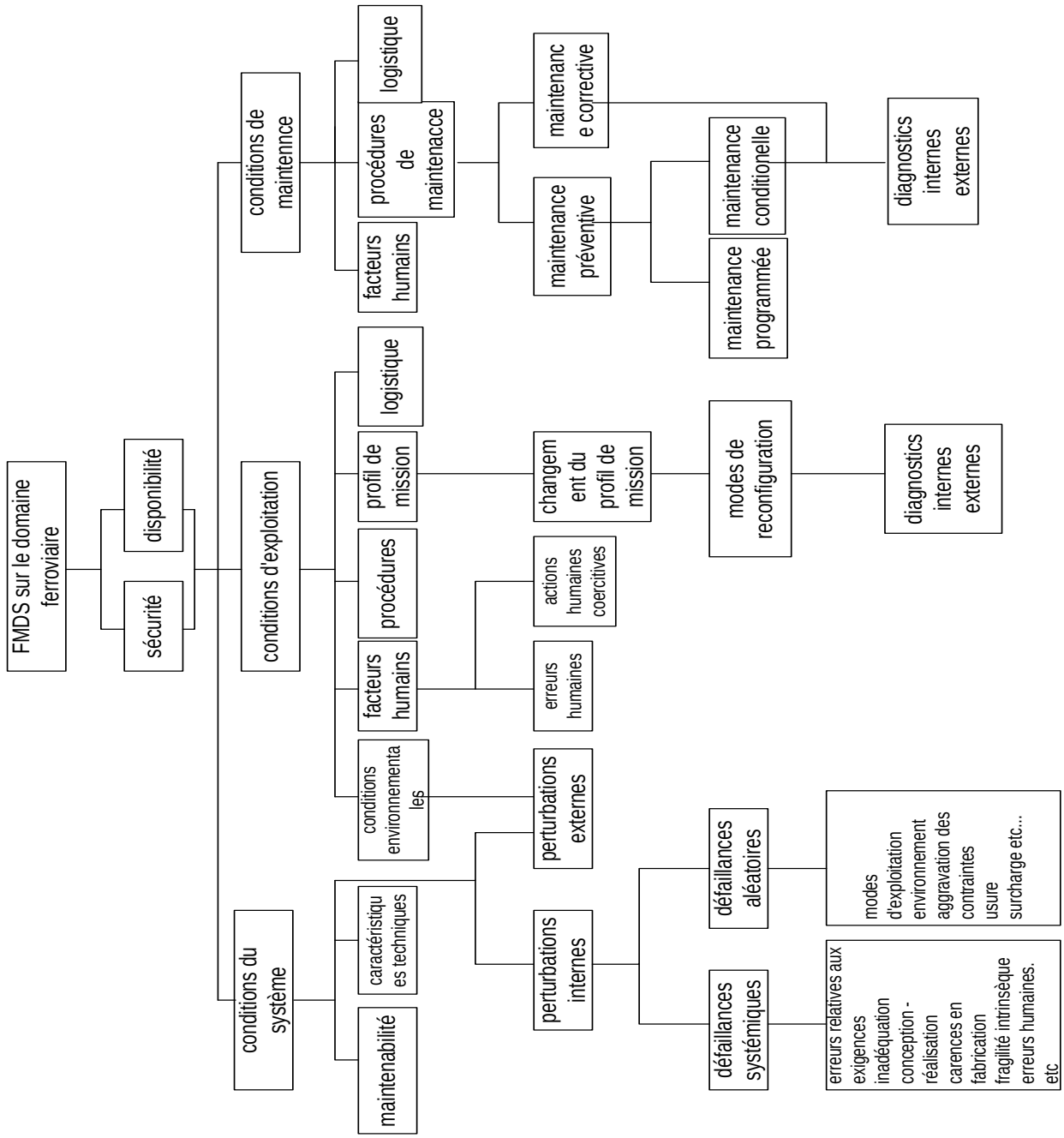


Figure 11 : décomposition des facteurs d'influence humains du risque ferroviaire [EN50126]

Les outils d'analyse des risques

Quel que soit le domaine, industriel ou technologique, les analyses de risques ont toutes pour objectif unique d'identifier l'ensemble des chemins pouvant conduire à des situations réputées dangereuses:

- Soit par l'analyse inductive, ou descendante, qui identifie les réseaux d'évènements (les coupes) conduisant à des situations dangereuses,
- Soit par l'analyse déductive, ou remontante, qui à partir des situations dangereuses identifie les évènements pouvant y conduire.

Qu'il soit inductif ou déductif, le processus réalise une analyse combinatoire visant à identifier des réseaux d'évènements. Une fois identifiés ceux-ci sont pondérés suivant leur probabilité d'occurrence et la gravité estimée des conséquences. Le couple (gravité – occurrence) devient alors le critère quantificateur du risque. La démarche d'acceptabilité du risque, ou la classification suit le processus décrit dans les paragraphes précédents pour définir l'effort à développer pour réduire le niveau de gravité des conséquences ou le niveau d'occurrence.

Différentes méthodes et différentes approches, décrites plus loin dans ce mémoire, sont employées pour l'identification des risques. Ces méthodes d'analyse peuvent être soit issues d'une démarche intellectuelle soit de calculs formels. La démarche intellectuelle, implique formalisme, itération et méthodologie mais est applicable au système en général. La démarche de calcul, s'appuie sur l'analyse systématique de comportements déterministes et déterminés, et est applicable à des systèmes purement technologiques.

L'analyse descriptive des risques porte sur l'information relative à la séquence événement – situation – conséquence, c'est-à-dire l'analyse des chaînes d'événements et situations conduisant à des conséquences dommageables dans un système ou sur les relations entre systèmes (respectivement sous systèmes). L'analyse descriptive dégage la morphologie du risque, la structure des relations entre les éléments d'un système et les événements qui conduisent aux conséquences dommageables. Ce type d'analyse fait appel à la théorie des graphes et en particulier aux arbres : arbres de causes, arbres de défaillances, arbres de défauts, arbres d'événements. Chacune de ces analyses répond à une préoccupation déterminée qui peut être résumée par le concept du nœud papillon développé par Shell [COUREAUNAU 2003]:

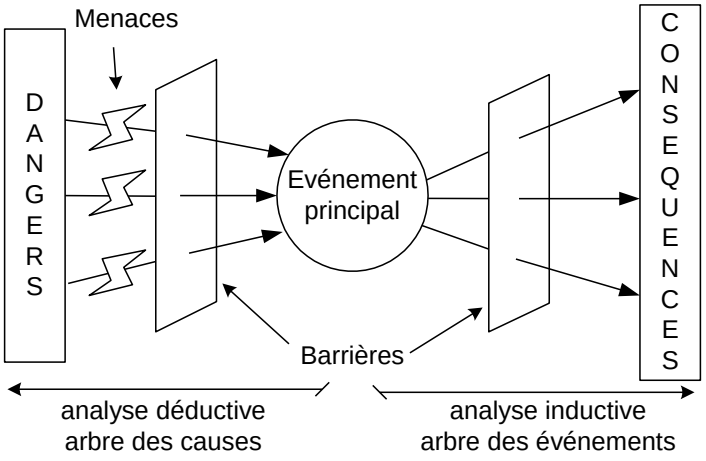


Figure 12 : nœud papillon de SHELL

Les différentes approches se répartissent en deux grandes classes :

- les analyses basées sur des outils méthodologiques,
- les analyses basées sur la théorie des graphes.

Les outils méthodologiques

L'APR, Analyse Préliminaire des Risques : La première étape de l'analyse des risques (l'analyse des dangers), doit identifier toutes les situations dangereuses raisonnablement prévisibles en les classant par ordre de priorité. Ces situations dangereuses seront celles résultant des fonctions et de l'exploitation normale du système dans son environnement, mais aussi celles relatives aux conditions de pannes, aux situations d'urgence ou dégradées, à la mauvaise utilisation du système ou de ses interfaces. La réflexion couvrira aussi les situations dangereuses induites par la maintenance, la dépose, les conditions naturelles ou industrielles de l'environnement, mais aussi, aux facteurs humains.

L'AMDE(C), Analyse des Modes de Défaillance de leurs Effets (et de leur Criticité) : Cette analyse des risques est avant tout une méthode statique d'analyse, s'appuyant sur un raisonnement inductif (causes - conséquences), pour l'étude organisée des causes, des effets des défaillances et de leur criticité. L'AMDEC a été employée pour la première fois à partir des années 1960 dans le domaine de l'aéronautique pour l'analyse de la sécurité des avions. La mise en œuvre s'est longtemps limitée à l'utilisation dans le cadre d'études de fiabilité sur du matériel. Bien qu'ayant subi de nombreuses critiques dues au coût et à la lourdeur de son application, elle reste néanmoins une des méthodes les plus répandues et l'une des plus efficaces. Elle est en effet de plus en plus utilisée en sécurité, maintenance et disponibilité non seulement sur le matériel, mais aussi sur le système, le fonctionnel et le logiciel. Dans le ferroviaire, la méthode a été expérimentée sur le logiciel critique dans le cadre de conduite automatique. Une adaptation de cette méthode a donné naissance à la méthode AEEL (Analyse des Effets des Erreurs du Logiciel) qui ressemble beaucoup à l'AMDEC.

Avant de se lancer dans la réalisation proprement dite des AMDEC, il faut connaître précisément le système et son environnement. Ces informations sont généralement les résultats de l'analyse fonctionnelle, de l'analyse des risques et éventuellement du retour d'expérience. Il faut également déterminer comment et à quel fin l'AMDEC sera exploitée et définir les moyens nécessaires, l'organisation et les responsabilités associées.

Il faut ensuite évaluer les effets des modes de défaillance à partir d'études conduites d'abord sur les composants directement interfacés avec celui-ci (effet local) puis de proche en proche (effets de zone) vers le système et son environnement (effet global). Il est important de noter que lorsqu'une entité donnée est considérée selon un mode de défaillance donné, toutes les autres entités sont supposées en état de fonctionnement nominal.

Enfin, il convient de regrouper et hiérarchiser les effets des modes de défaillance par niveau de criticité relativement aux critères de sûreté de fonctionnement préalablement définis au niveau du système (fiabilité, sécurité, etc.). Cette typologie permet d'identifier les composants les plus critiques et de proposer alors les actions et les procédures " juste nécessaires " pour y remédier. Cette activité d'interprétation des résultats et de mise en place de recommandations constitue la dernière étape de l'AMDEC.

Bien que simple, la méthode s'accompagne d'une lourdeur certaine et la réalisation exige un travail souvent important et fastidieux. Une des difficultés réside dans l'optimisation de l'effort

entre le coût de l'analyse AMDEC (dépendant de la profondeur de l'analyse) et le coût de l'amélioration à apporter. La solution pour surmonter le volume des entités à étudier est de conduire des AMDEC fonctionnelles. Cette approche permet de détecter les fonctions les plus critiques et de limiter ensuite l'AMDEC " physique " aux composants qui réalisent tout ou partie de ces fonctions.

La **MCPR, Méthode de Combinaison des Pannes Résumées** : Cette méthode est un prolongement de l'AMDE qui ne traite que les effets de défaillances uniques. La démarche est exactement de même nature (inductive) et a pour objectif d'appréhender les effets de combinaisons de défaillances menant aux mêmes conséquences. MCPR effectue une synthèse de l'AMDE(C) et réalise un processus de réduction logique de regroupements de pannes à travers la démarche suivante :

- Toutes les Pannes Résumées Internes, ou PRI, et toutes les Pannes Résumées Externes, ou PRE, sont recensées à partir de l'AMDE de chaque système élémentaire. Par PRI, s'entendent les regroupements de pannes affectant d'autres systèmes élémentaires. Par PRE, on comprend les regroupements de pannes provenant d'autres systèmes et affectant le système analysé. Les critères formels de regroupements sont que deux modes de défaillances distincts menant aux mêmes effets doivent voir toute combinaison logique de ces modes avoir les mêmes effets. Si une combinaison quelconque de ces modes n'a plus le même effet, il faut alors distinguer deux PRI.
- Après avoir déterminé les PRI et les PRE, la démarche d'élaboration des Pannes Résumées Globales établit les combinaisons de PRI et PRE ayant les mêmes effets sur les systèmes élémentaires.

La méthode permet une analyse combinatoire des différents modes de défaillances identifiés pendant l'AMDE, mais la quantification des modes résultants ne peut être effectuée qu'avec d'autres méthodes telles l'arbre des causes.

L'analyse des conditions insidieuses (sneak analysis) : Sneak Analysis est une méthodologie utilisée pour identifier les défaillances qui peuvent trouver leur origine dans la conception d'ensemble. Il ne s'agit pas ici de recherche des erreurs de conception fonctionnelle mais plutôt de rechercher des erreurs de conception ou d'opération tels que des modes communs de défaillances de systèmes élémentaires redondants, … Parmi les conditions insidieuses, il est possible de citer rapidement :

- L'erreur d'interprétation du à une signalétique ambiguë, un même symbole avec un sens différent suivant l'installation, une représentation inadaptée aux conditions d'environnement,
- Une indication inappropriée, une fréquence de clignotement inadaptée au délai de réaction,
- Des séquences conflictuelles comme un positionnement de commande incohérent avec la séquence à effectuer. Par exemple, la mise en route du système de ventilation forcée du métro de Hong Kong, pour lequel la société en charge de la programmation des automates n'avait reçue aucune spécification sur les séquences opérationnelles et avait initialisé les tables dans l'ordre alphabétique des équipements ; au premier démarrage, les ventilateurs ont été mis en route avant l'ouverture des clapets d'admission d'air ce qui a conduit à la déformation des conduites.
- Une procédure insidieuse qui caractérise la prise en compte d'un événement survenant au mauvais moment, sur un délai trop long, ou en conflit avec une séquence. Le problème est souvent dû au flou laissé par une procédure ou par l'officialisation d'un mauvais comportement n'ayant jamais eu de conséquence mais devenu habituel. Nous vivons ce phénomène quotidiennement, par exemple la mise en place d'une phase de

"rouge intégral" aux carrefours pour couvrir les franchissements à l'orange fréquents et qui "pousse" l'usager à continuer à passer.

- L'erreur de contrôle, due à une indication fausse ou ambiguë, par exemple pour l'accident du DC10 de Turkish Airlines à Ermenonville où l'indication de fermeture de porte n'était pas couplée au bon enclenchement de la gâche mais à la manœuvre du levier de verrouillage.
- L'apparition de couplages ou circuits virtuels, comme par exemple un fluide remontant un circuit pour un problème de différence de pression. Ce type de condition a contribué à l'incident de Three Mile Island.
- Enfin, car récente et catastrophique, la réaction imprévue comme la mise en présence de produits réactifs et du catalyseur de la réaction comme à Toulouse en septembre 2001.

Ce type d'analyse impose un regard de compétences différentes à celle du concepteur du composant, par exemple pour analyser les effets de radiations sur les matériaux utilisés sur un équipement conçu par un électronicien.

L'Analyse Pire Cas est essentiellement utilisée pour évaluer la marge de bon fonctionnement d'un équipement ou d'un composant électronique jugé critique sur un environnement donné. L'APC demande une connaissance fine du fonctionnement de l'équipement ou composant et une analyse statistique et probabiliste de la variation des paramètres du domaine sur lequel il évolue. Trois méthodes sont utilisées pour l'évaluation :

- les valeurs extrêmes qui utilise directement les valeurs limites des paramètres. La méthode est simple et rigoureuse mais pessimiste et majorante. L'intérêt de cette méthode est qu'une simple vérification peut permettre de démontrer que la marge reste correcte sur la totalité du domaine sans restriction.
- La méthode de Monte Carlo qui permet d'obtenir une distribution statistique de bon fonctionnement pour chaque paramètre sur le domaine et d'en déduire une loi de bon fonctionnement.
- La sommation quadratique qui consiste à séparer pour chaque valeur d'entrée le biais de la mesure de la part aléatoire du comportement.

Les outils issus de la théorie des graphes

L'arbre des événements, permet à partir d'une liste d'événements et de fonctionnement attendus du système observé de construire un ensemble de situation d'arrivée (ou scenarii). En pondérant chaque réponse du système par une probabilité, on obtient alors une probabilité d'occurrence des situations. C'est une méthode d'analyse inductive.

L'arbre des cause, ou arbre des défaillances, nommée aussi Fault Tree Analysis, méthode déductive, permet de déterminer les causes d'une situation par l'analyse remontante des défaillances successives qui ont pu y conduire. Le modèle des arbres de défaillance est utilisé pour représenter les états de dysfonctionnement du système. Chaque étape de la construction consiste à raffiner la défaillance par un raisonnement déductif qui détermine quelles combinaisons d'événements contribuent à cette défaillance. Les combinaisons sont exprimées à l'aide d'opérateurs booléens (pour la plupart) .Ce processus est itéré jusqu'à la granularité souhaitée ; les événements terminaux (les feuilles de l'arbre) sont supposés indépendants au sens des probabilités. Cette méthode produit un arbre dont les sommets sont affectés d'une représentation symbolique suivant le type d'événement et le type de condition sur les séquences d'événements. Chaque nœud de l'arbre est le résultat d'une formule booléenne dont les variables sont les feuilles. Ces feuilles représentant la défaillance des composants. De même, l'affectation d'une variable statistique ou d'un estimation probabiliste à chaque défaillance élémentaire permet de calculer la

probabilité de chaque nœud. Cette méthode est très utilisée en électronique ou les modes de défaillances des composants sont connus, indépendants entre eux et quantifiables en probabilité.

Les Block diagrams ou diagrammes de succès modélisent les conditions de bon fonctionnement du système ou de réalisation d'une de ses fonctions. Chaque nœud représente un composant du système et chaque arc représente une dépendance de fonctionnement entre les composants. Le bon fonctionnement du composant ou la bonne réalisation de la fonction conditionnant le parcours, le chemin parcouru est alors appelé chemin de succès.

Les réseaux bayésiens : les réseaux bayésiens reposent sur un formalisme issu de la théorie des graphes et des probabilités. Un réseau bayésien permet de représenter un ensemble de variables aléatoires pour lesquelles on connaît un certain nombre de relations de dépendances. Ces réseaux établissent une représentation graphique de la causalité entre les événements, les probabilités permettent d'évaluer l'occurrence sur les nœuds en fonction des racines, des distributions locales aux nœuds et des probabilités conditionnelles associées aux relations de cause à effet représentées. Ces réseaux permettent une circulation de l'information, c'est-à-dire que toute nouvelle information rajoutée va en modifiant la probabilité locale de certains nœuds modifier l'ensemble du réseau. L'intérêt de ces réseaux est de permettre une analyse inductive (mesure de l'impact d'un évènement sur le réseau) et déductive (examen des causes les plus probables conduisant à un nœud).

En complément de l'analyse descriptive il peut être nécessaire de suivre les évolutions d'un système dans le temps en étudiant les différentes transitions entre les divers états du système. C'est l'objectif de méthode dynamiques telle que :

Les processus de Markov : les processus de Markov sont un cas particulier des processus stochastiques. En modélisation de Markov, pour décrire l'évolution d'un système dynamique, la méthodologie consiste à définir un espace d'états dans lequel se promène le système ; une chaîne de Markov est un automate à *n* états pour lequel on calcule la probabilité de transition d'un état à un autre mais aussi la probabilité que l'automate soit dans un état donné à un instant donné. La théorie des processus de Markov permet alors de calculer les probabilités d'état stationnaires qui sont des états vers lequel tend le système au cours du temps. Etant donné qu'un processus Markovien est un processus homogène dans le temps, cette méthode est utilisable pour l'analyse de système dont les conditions de changement d'état sont indépendantes du temps.

Les méthodes de Monte Carlo : La méthode de Monte-Carlo permet d'évaluer les caractéristiques d'un processus stochastique (moyenne, variance, … des variables aléatoires) en simulant le comportement des phénomènes décrits par les variables aléatoires au cours du temps. Deux approchent existent :

- L'implémentation d'un algorithme de simulation ad hoc construit directement à partir de la structure et des composants physiques du système;
- L'utilisation d'un algorithme générique construit à partir d'un modèle de comportement; par exemple les réseaux de Pétri. Le modèle définit les règles du *jeu* nécessaires à la simulation. L'algorithme de simulation peut alors être appliqué à n'importe quel type de système (dès lors qu'il est modélisé en utilisant le formalisme choisi).

Cette méthode est fréquemment rencontrée lorsque :

- Le processus stochastique est markovien mais l'ensemble des états est trop important pour être stocké ou pour appliquer les méthodes analytiques usuelles ;
- Le processus est non markovien ce qui interdit l'utilisation des méthodes analytiques.

La réduction des risques en phase conception et réalisation

On ne parle jamais de suppression du risque mais de réduction ou parfois de couverture du risque. Pour les situations inadmissibles, la démarche de réduction intervient alors :

- soit sur le réseau d'évènement lui-même pour l'interrompre ou le dévier,
- soit sur la probabilité d'occurrence d'un évènement du réseau, de façon à rendre le risque final admissible,
- soit sur le critère de gravité, par protection, c'est-à-dire en interposant une barrière, ou par éloignement des victimes potentielles).

Quelque soit l'approche ou la méthode choisie l'analyse des risques est conduite sur un système dont les limites sont connues et définies : composants, architecture, contexte, intervenants…Seules des différences méthodologiques apparaissent dans la mise en œuvre des analyses et dans la façon d'appréhender le cycle de vie, le contexte ou les intervenants sur le système. Une des limites essentielles de ce type de processus est que pour être efficace et admissible il est nécessaire que l'analyse soit la plus exhaustive possible. Qu'elle soit empirique ou systématique, l'analyse tente d'épuiser l'ensemble des cas, coupes ou évènements, de façon à garantir la maîtrise de la situation (et non de l'évènement). Au-delà d'une certaine complexité du système, seules les machines peuvent identifier la totalité des réseaux d'évènements. Cependant pour fonctionner les logiciels ont besoin que la description du système soit formalisée et codée pour être exploitable. L'analyse se heurte alors à deux facteurs non négligeables, la distorsion apportée dans la description du système, et le coût de l'opération.

La théorie de la conception des installations de sécurité s'est bâtie progressivement, avec une évolution continue, autour d'une approche démonstrative. Dans le ferroviaire, avec les premières installations mécaniques de signalisation sont apparues les notions de sécurité intrinsèque et de sécurité par redondance. Ces notions se sont ensuite précisées pour devenir des règles formelles dans les installations électromécaniques et dans les premiers équipements électroniques. Cette évolution continue a permis aux techniciens de résoudre des cas de plus en plus compliqués, de s'adapter à une technologie nouvelle (semi-conducteurs en éléments discrets) sans remettre en cause la notion implicite de sécurité. L'expérience a montré que malgré la multiplication du nombre d'installations, le nombre d'incidents n'a pas significativement augmenté. Néanmoins l'approche démonstrative a pour objectif essentiel de prouver qu'une défaillance de l'équipement ne conduit pas à une situation dangereuse. Pour cette raison, les démonstrations de sécurité sur le domaine purement technologique sont essentiellement tournées vers la couverture des défaillances. La sécurité se définie alors comme l'aptitude d'un dispositif à traduire toute défaillance de l'un quelconque de ses éléments constitutifs, par une information de sortie plus restrictive (ou moins permissive) que celle qui aurait été délivrée en fonctionnement normal. Une défaillance est un événement qui place au moins une caractéristique d'un composant hors des limites spécifiées. Cette dernière définition est intéressante car elle présente une défaillance non pas comme un arrêt d'un composant ou une mauvaise information de sortie, mais aussi comme le fait de sortir des spécifications. L'application des principes de la sécurité conduit à une option beaucoup plus tranchée, c'est à dire que l'apparition de toute défaillance se traduit par :

- La disparition immédiate de l'information de sortie si celle-ci était normalement présente,
- La non apparition de l'information de sortie si celle-ci devait normalement apparaître.

En final, la défaillance va se traduire par l'arrêt d'une installation, ou par le maintien dans une position dite sécuritaire de l'équipement terminal. Le contrôle de la sécurité d'un appareil repose sur les hypothèses suivantes :

- Les défaillances admises comme possibles doivent être clairement répertoriées.
- Les défaillances doivent être rapidement détectées.
- Deux défaillances indépendantes ne peuvent se produire simultanément. Les notions de rapidité et simultanéité étant relativement vague, ce principe s'énonce alors comme la probabilité que deux défaillances indépendantes successives survenant pendant le temps de latence de la détection soit négligeable.
- Les défaillances dont le temps de latence est important doivent être examinée en association avec toutes les autres défaillances reconnues possibles.

Ces règles s'appliquent aux défaillances indépendantes simples comme aux défaillances corrélées. Pour obtenir une détection rapide des défaillances, les méthodes suivantes sont alors utilisées :

- Contrôle cyclique de l'état des circuits,
- Travail dynamique, méthode très utilisée dans les systèmes de sécurité intrinsèques (par exemple la pompe à diode, convertisseur créneaux – tension continue, est un circuit passif dont l'énergie en sortie dépend uniquement de l'énergie fournie en entrée),
- La redondance des traitements des informations de sortie.

Les diverses techniques utilisées pour détecter une défaillance doivent aboutir au même résultat pour la sécurité.

Les systèmes de sécurité intrinsèque

Pour les chemins de fer, les systèmes électroniques dits de sécurité intrinsèques comportent un chemin unique de traitement équipé de composants maîtrisés, utilisés dans un domaine de spécifications mécaniques, climatiques et électriques précises. Les composants utilisés sont ceux dont les défaillances admises comme possibles, sont répertoriées dans des catalogues de défaillances et des normes reconnues. Seul le respect de ces conditions autorise l'analyse et la vérification systématique de la réaction des matériels aux défaillances. Ces équipements à chemin unique de traitement de sécurité intrinsèque ont été largement développés par l'industrie française, non seulement dans le domaine ferroviaire mais aussi dans l'industrie du nucléaire dont les systèmes de contrôle doivent également posséder un état restrictif sûr. Ces circuits sont souvent associés à un relais de sécurité qui délivre l'information de sortie de façon à s'intégrer dans les schémas classiques de l'électromécanique.

Les systèmes redondants contrôlés

Ces systèmes utilisent plusieurs chemins de traitements, non de sécurité intrinsèque, utilisés en redondance. La sécurité globale est obtenue par un contrôle de vraisemblance des informations de sortie. Ce principe permet d'utiliser des composants pour lesquels les règles définies au paragraphe précédant ne sont pas applicables, les circuits intégrés digitaux en particulier. La redondance peut être physique, le principe consiste alors à faire effectuer les traitements par au minimum deux chaînes indépendantes, le plus souvent en parallèle dont les résultats de sortie sont comparés puis validés par un circuit de sécurité intrinsèque. Pour éviter les modes communs, les chaînes sont diversifiées dans leur alimentation, leurs composants, leur logique et leur base de temps. La redondance peut aussi être sur l'information, dans ce cas les états logiques de sortie des diverses chaînes sont surveillés en dehors des changements d'états. Il s'agit de vérifier par l'analyse que l'ensemble chaînes et comparateur a un comportement global de sécurité intrinsèque. Le principe de la sécurité par redondance a beaucoup été appliqué dans les chemins de fer allemands dont les circuits électromécaniques comportaient déjà une redondance de circuits complémentaires qui permettaient d'utiliser des relais dont la seule contrainte était que

les contacts soient non chevauchants. En France, ce principe a peu été utilisé dans les installations de signalisation, sauf pour des cas particuliers comme les pédales d'annonce de train aux passages à niveau. Pour bien comprendre la problématique du contrôle redondant, il est intéressant de développer un peu cet exemple. La Figure 13 suivante montre le principe de base du système d'annonce à pédales électromécaniques. Ces pédales sont doublées pour se prémunir contre le risque de rupture du bras de commande des contacts. De plus, pour éviter le mode commun que représente une rupture simultanée des deux bras par une pièce traînante, les pédales ne sont pas montées sur la même file de rail. Toutefois ce montage n'est pas entièrement satisfaisant car la rupture d'un seul bras n'est pas détectée ; le temps de latence de la détection dépendra alors de la fréquence de maintenance des pédales.

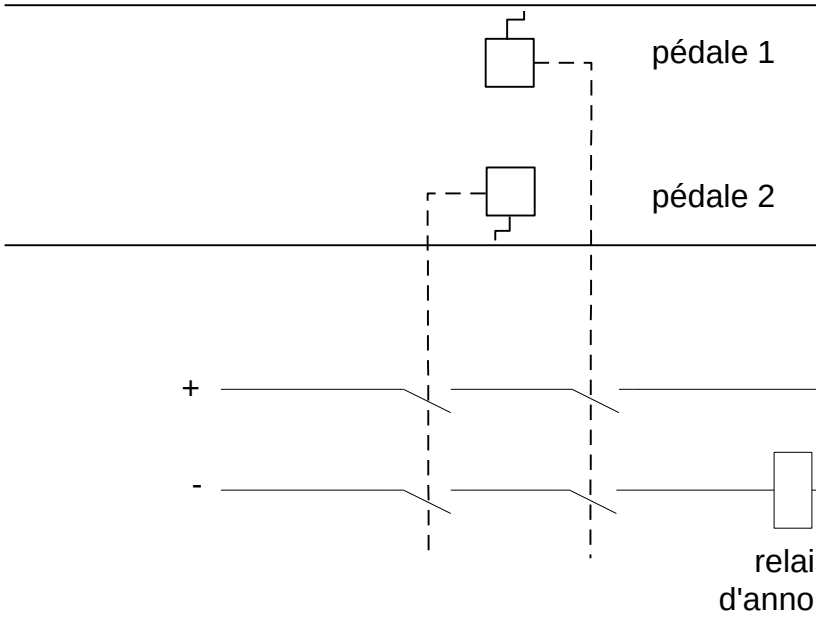


Figure 13 : système d'annonce à redondance

En généralisant ce montage comme la sortie d'une porte ET sur l'information fournie par chaque pédale, nous obtenons la table de vérité suivante :

Pédale 1	Pédale 2	Sortie S	
0	0	0	Annonce normale d'un train
0	1	0	Avarie sur pédale 2 figée à 1
1	0	0	Avarie sur pédale 1 figée à 1
1	1	1	Etat de veille

Ce tableau montre bien que le contrôle d'identité des deux sorties n'est pas effectué et qu'il n'y a pas de détection de la présence permanente d'un 1 sur l'une ou l'autre des chaînes de traitement de l'information. La seule redondance physique des chaînes de traitement ne suffit donc pas pour respecter une des règles de la sécurité qui veut que toute défaillance soit rapidement détectée.

L'utilisation de pédales électroniques permet de pallier ce problème en effectuant un contrôle de cohérence sur les sorties S et non S.

Les catalogues de défaillances

Les catalogues de défaillances représentent un outil à mi chemin entre le retour d'expérience et les règles formelles de conception et de réalisation. Ces catalogues très utilisés en signalisation ferroviaire ont pour origine les premiers temps de l'utilisation des semi conducteurs, où les hypothèses de pannes reconnues possibles se résumaient à des coupures ou à des courts-circuits. Quelques incidents contraires à la sécurité ont montré, après une expertise minutieuse des équipements en défaut, que les défaillances des composants avaient pour origine des modes non pris en compte jusque là ; en particulier, les pannes intermittentes et les comportements intermédiaires pouvant précéder une panne franche : augmentation de la valeur de résistance série avant coupure, ou augmentation du courant de fuite avant un court-circuit. Très rapidement les différents réseaux de l' Union Internationale des Chemins de fer qui utilisaient des composants électroniques ont confronté leurs positions en ce domaine pour aboutir à un catalogue des défaillances commun qui est devenu ensuite la norme européenne EN50129 [EN50129]. Toute conception électronique de sécurité doit prendre en compte la réaction des équipements aux défaillances reconnues comme possible. Cette analyse conduite théoriquement en phase de conception, le composant produit est ensuite vérifié à partir d'une campagne d'essais systématiques préalables à toute homologation.

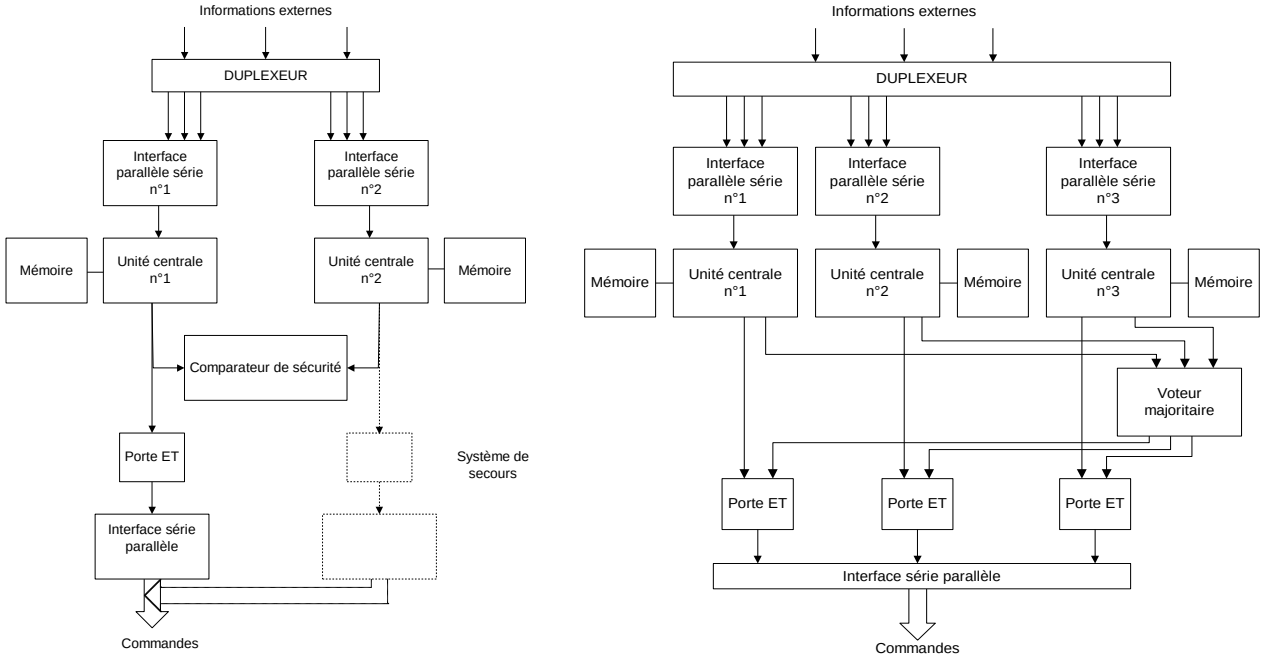
Dans le même esprit les bases de données sur les composants sont très utilisées en conception électronique, en particulier dans les analyses de fiabilité. Les plus connues, le Military Handbook 217 [MILH 1995] et le recueil de fiabilité du Centre National d'Etudes des Télécommunications (CENT) [CNET 1993] permettent de calculer le taux de fiabilité des composants en fonction des caractéristiques de l'application (environnement, facteur de marche, taux de charge…) et des caractéristiques du composant (nombre de portes, valeur de résistance…). L'électrotechnique et la mécanique ont-elles aussi de tels recueils ou ouvrage contenant des méthodes de calcul, citons : "Utilisation des techniques de fiabilité en mécanique" de C. Marcovici et JC Ligeron, [LIGERON 1974] ou l'IEEE STD 500 [IEEE 1984]: recueil concernant les composant électroniques, électriques et mécaniques pour les centrales nucléaires.

Sécurité et logiciel

Les approches décrites précédemment ont surtout pour objectif de sécuriser les chaînes de contrôle et de commande de bas niveau réalisables avec des équipements mécaniques, électromécaniques ou électroniques. L'augmentation des besoins en performances a impliqué dans un premier temps d'automatiser des fonctions de contrôle-commande plus complexes et surtout d'automatiser les chaînes de décision. Ce travail a été rendu réalisable par l'introduction du logiciel. Or sécuriser les équipements fonctionnant essentiellement à partir de logiciel oblige à considérer trois niveaux différents de défaillance : la défaillance en conception, la défaillance en exécution qui peut elle-même être causée par une défaillance logicielle mais aussi du processeur sur lequel est exécuté le programme. Pour sécuriser du logiciel il est donc nécessaire de traiter la conception, l'outil de programmation mais aussi le produit réalisé.

Compte tenu du caractère non déterminé des défaillances des microprocesseurs et des codes qu'ils supportent, il a fallu concevoir une architecture matérielle adaptée. Une première approche consiste à concevoir une architecture redondante en couplant deux microprocesseurs sur un comparateur de sécurité intrinsèque (réalisé avec des composants discrets). Ce principe a

rapidement évolué, pour des raisons de disponibilité, vers l'utilisation d'un troisième microprocesseur ; dans ce cas le comparateur est remplacé par un voteur à logique majoritaire qui délivre l'information issue d'au moins deux microprocesseurs.



Architecture à deux microprocesseurs et comparateur

Architecture à trois microprocesseurs et voteur

Figure 14 : Types d'architectures redondantes multiprocesseurs

La conception de tels systèmes programmés est basée sur une redondance matérielle qui consiste à utiliser plusieurs calculateurs en parallèle et à effectuer des comparaisons de résultats. Dans un tel système, la sécurité repose sur la connaissance des calculateurs, pour effectuer des autocontrôles et des contrôles croisés, et, sur l'élimination des pannes de mode commun (une même cause ne doit jamais affecter les calculateurs simultanément). De plus, la synchronisation des calculateurs reste difficile à réaliser.

Le processeur codé

Le transport ferroviaire a préféré à la redondance matérielle une autre méthode permettant d'assurer la sécurité uniquement par un codage approprié des informations traitées alors dans un seul processeur (appelé « monoprocesseur codé »). Elle a été développée au début des années 1980 à partir d'une idée de Matra Transport. Le choix de ce type d'approche est motivé par le postulat de départ qui est que pour assurer la sécurité du système, il faut détecter tous les dysfonctionnements et les erreurs pouvant se produire entre l'écriture du code source logiciel et l'exécution de ce logiciel dans l'équipement et que ces défaillances se ramènent toujours à une combinaison des trois cas suivants :

- erreur d'**opérande** (mauvais adressage ou non rafraîchissement. On fait un calcul en utilisant des valeurs de départ incorrectes)
- erreur d'**opérateur** (mauvais adressage ou mauvais décodage. On se retrouve, par exemple, à faire une addition au lieu d'une multiplication)
- erreur d'**opération** (mauvaise valeur. Les données du calcul étaient correctes, mais le résultat est faux)

L'approche consiste donc à coder chaque valeur traitée par le processeur en une partie "information" et une partie "contrôle". Cette méthode associe deux techniques de codage :

- un code arithmétique, détectant les erreurs affectant les informations en mémoire, les transferts d'informations, et les erreurs lors de la manipulation d'informations (instructions mal exécutées) ;
- une signature, décelant les erreurs de fonctionnement du programme.

A partir du programme source, le processeur codé peut détecter toutes les défaillances de la chaîne de traitement, depuis la compilation jusqu'à l'exécution du programme, sans vérification préalable des outils intermédiaires (compilateur, assembleur, ...). Le contrôle de bon fonctionnement du programme s'effectue sur les variables de sortie qui contiennent l'historique de leur génération. Ce contrôle doit être de sécurité et ne peut donc être exécuté qu'en sécurité intrinsèque. La partie de contrôle de la ou des variables de sortie est transformée en séquence de bits. Cette séquence et la date sont émises bit à bit vers un contrôleur dynamique constitué principalement de OU exclusif de sécurité qui compare la séquence avec une référence contenue dans une mémoire morte. Dès qu'un défaut est détecté, le contrôleur chute, entraînant en sécurité le positionnement à l'état restrictif de toutes les sorties.

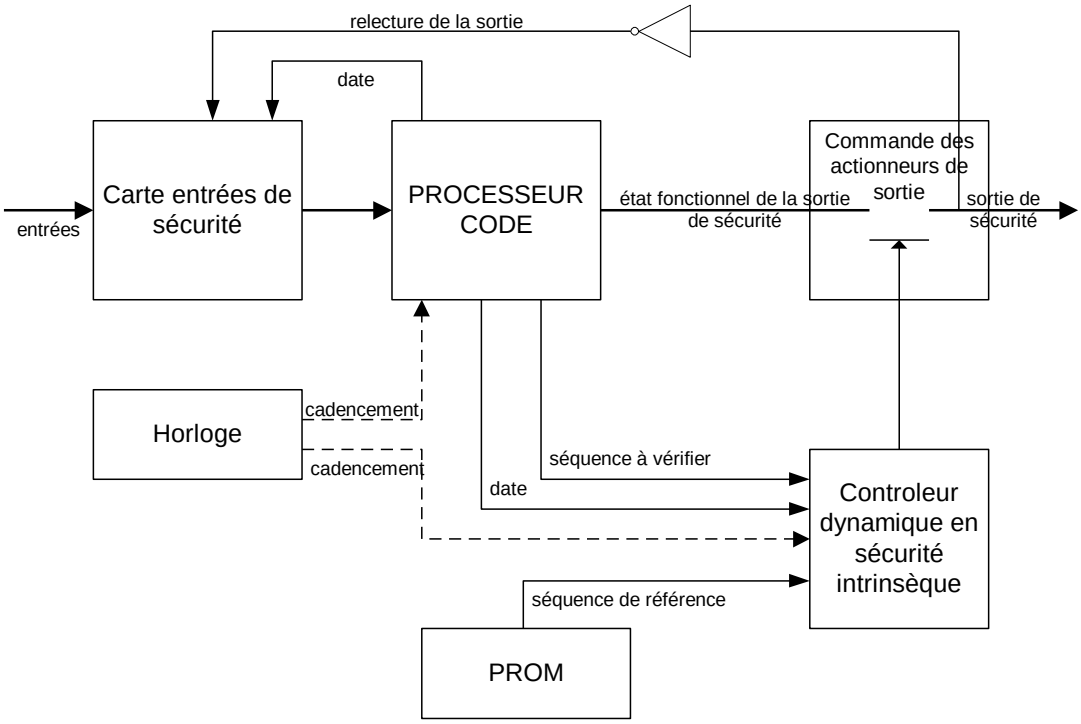


Figure 15 : Schéma de principe de contrôle de code

De plus, le codage qui est à la base de cette solution technique permet aussi de détecter les erreurs dans la transmission des informations.

Les méthodes formelles

Toutes les techniques qui viennent d'être abordées couvrent les risques dû à une défaillance de l'instruction. Ces techniques ont le même objectif que les méthodes de couverture des risques de défaillance des équipements mécaniques, électromécanique ou électroniques qui obéissent à des lois physiques indépendantes du concepteur et du réalisateur. Or, dans le domaine du logiciel, l'expression appartient plutôt au domaine du langage. En particulier, la même fonction peut se décrire et s'implémenter de façon différente suivant qui la spécifie ou qui la réalise. La

démonstration de sécurité est alors confrontée au problème de l'individualisation du composant, c'est à dire que ses propriétés comportementales ne sont plus déterminées.

Les méthodes formelles permettent à un créateur de logiciel de prouver mathématiquement les propriétés et la validité du logiciel. La méthode repose sur une approche d'analyse logique propositionnelle, qui permet de modéliser, à des fins de vérification ultérieure, tout système logiciel où les variables sont finies et définissables. Le principe des méthodes formelles est d'exprimer à partir d'une base axiomatique les propriétés d'un système. Le langage formel ainsi défini est utilisé pour la construction de spécifications afin de réduire la part de l'intuition humaine dans leur interprétation. Les axiomes fournissent tout ce qui pourra être exprimé par l'objet spécifié. Dans le cas où les spécifications possèdent des propriétés non décrites explicitement dans ces axiomes, celles-ci doivent être des conséquences logiques de ces axiomes. L'utilisation de méthodes formelles permet de concevoir des modèles de spécification sur lesquels il est possible d'effectuer directement la validation du logiciel (par plusieurs méthodes: simulation, vérification ou même démonstration). Le développeur part d'un modèle réputé sûr, la cohérence du modèle, puis la conformité du programme final par rapport à ce modèle étant garantie par des preuves mathématiques. La démonstration de ces preuves dans un cas concret ne peut s'envisager que grâce à l'utilisation d'outils de preuve automatiques,

Une des méthodes formelles utilisée dans les systèmes de transport est la méthode B. Cette méthode a été introduite dans le développement de logiciels par la RATP qui était confrontée à la nécessité de concevoir des systèmes de plus en plus complexes évoluant vers la marche en automatique des trains, en sécurité. Le concept de base est celui d'une machine abstraite dont l'état est décrit par un invariant. La méthode consiste à prouver formellement que les opérations respectent bien l'invariant, puis à raffiner les machines abstraites en machines implantables, et à prouver que ce raffinage est correct. Le raffinage peut également être utilisé comme technique de spécification. Dans ce cas, le raffinage permet d'inclure petit à petit les détails du problème dans le développement formel. La spécification formelle est alors réalisée progressivement et non pas directement. En final, la validité du logiciel est ainsi prouvée par construction relativement à sa spécification. La méthode utilise une notation fondée sur les concepts mathématiques de la théorie des ensembles. L'existence d'une notation utilisable tout au long du développement offre un cadre formel uniformisé allant de la spécification et la conception jusqu'à la réalisation des composants logiciels exécutables sur lequel il est possible de conduire des démonstrations à partir d'outils automatiques.

Les langages formels pour l'implémentation logicielle

L'intérêt des méthodes formelles est de pouvoir construire un modèle de spécification sûr. Il reste donc nécessaire ensuite de faire appel à une implémentation conservant le niveau de fiabilité atteint, soit par le choix d'une des technologies matérielles décrites dans les paragraphes précédents, soit par le choix de langages établis sur le même formalisme, à savoir des jeux d'instructions et des mécanismes qui par leur sémantique permettent de détecter les incohérences et les situations de conflits latentes : réaction en chaîne, blocage, problème de cadencement… Les développements de composants logiciels restent contraints par le type de mécanisme à implémenter et par le fait que pour être sûr un composant logiciel doit être parfaitement déterminé.

Concevoir un langage (et un environnement) de programmation capable de répondre à ces contraintes pourrait sembler appartenir à la plus pure utopie toutefois des solutions existent. De plus, si dans certaines applications industrielles le niveau de sécurité peut être suffisant (ou l'objectif recherché peut être un niveau de fiabilité des résultats suffisant), la sécurité ultime est

toujours assurée par un composant de bas niveau réalisé en sécurité intrinsèque ou en sécurité contrôlée.

Ci-dessous sont brièvement décrits des langages de programmation conçus pour la conception, la vérification et l'implantation de systèmes réactifs. Cette notion de programme réactif a été introduite par D. Harel [HAREL 1985] pour décrire les systèmes dont l'interaction avec l'environnement contraint fortement le comportement; les systèmes de contrôle (commandes de vol par exemple) sont de ce type. Compte tenu de la forte implication de l'environnement dans le comportement du programme et inversement, il est nécessaire de sécuriser le comportement du logiciel en sécurisant l'écriture comme l'exécution.

Les langages qui le permettent se partagent en deux familles : les langages synchrones et les langages asynchrones. Le synchronisme est pris sur l'information sur laquelle réagit le programme. Chaque information en entrée susceptible de provoquer une réaction est considérée comme un signal; dans les langages réactifs asynchrones chaque action peut être interrompue alors que dans les langages réactifs synchrones toutes les actions sont terminées avant le traitement du signal suivant. Cette hypothèse n'est acceptable qu'à partir du moment où le système réagit infiniment plus vite que son environnement. Cette approche synchrone a été proposée par G. Berry [BERRY 1992] pour le développement d'ESTEREL. G Berry pose que la réaction d'un système réactif à son environnement est instantanée. En d'autres termes, l'ensemble des actions effectuées par le système pour répondre à son environnement s'effectue dans un intervalle de temps nul.

Ces langages permettent à partir d'outils d'effectuer des vérifications formelles sur les composants écrits. Même si ces langages ont été conçus par des équipes différentes, une relative universalité des sémantiques choisies et une mutualisation des recherches ont permis le développement d'outils partageables et interconnectables pour l'écriture et la vérification de programmes.

Comme exemples de langages asynchrones citons :

ELECTRE qui permet la programmation du noyau réactif d'applications temps-réel constituées d'un ensemble de modules (tâches) qui s'exécutent en parallèle. Chaque module est un code séquentiel ne comportant pas de point de synchronisation. Ces modules sont contrôlés (démarrage, interruption ou reprise) par un exécutif temps-réel offrant des facilités pour l'implémentation et la manipulation de tâches concurrentes. Le langage est doté d'opérateurs pour composer les modules mais aussi pour définir des structures d'événements qui représentent des activations de modules sur l'occurrence d'un événement.

STATECHARTS : Les statecharts définis par D. Harel [HAREL 1987] représentent un des premiers formalismes graphiques pour la modélisation de systèmes réactifs. Son originalité provient de la représentation graphique du parallélisme, de la concurrence et de la hiérarchie. Un statechart est un automate dont les états peuvent contenir un ou plusieurs automates (représentant ainsi un sous-système ou une sous-fonction du système global). Les statecharts ont séduit et font références dans toutes les démarches pour la représentation graphique des comportements des systèmes.

Comme exemples de langages synchrones citons :

ESTEREL : langage impératif s'appuyant sur un jeu d'une quinzaine d'instruction de base. Toutes les instructions complémentaires voient leur sémantique reposer sur ces instructions de base. Ce langage, commercialisé à travers l'atelier SCADE, est en application dans l'aéronautique.

LUSTRE et SIGNAL langages synchrones permettent de décrire un modèle par une hiérarchie de nœuds ou chaque sortie s'écrit comme une équation (pour LUSTRE) ou une relation

(pour SIGNAL) sur les entrées. Une horloge fournit la base de temps cadençant les flots de données parcourant le modèle.

ARGOS, langage graphique inspiré des statecharts et basé sur la notion d'automate. Ce langage permet la description de comportements non déterministes. Un système est représenté sous forme d'une hiérarchie d'automates à entrées/sorties.

SYNCCHARTS, formalisme graphique lui aussi inspiré des statecharts, développé par C. André [ANDRE 1996], et dédié à la modélisation de systèmes réactifs. SYNCCHARTS permet l'écriture de systèmes réactifs et de programmations synchrones.

Le couplage d'un formalisme SYNCCHARTS avec le langage ESTEREL permet de répondre à la problématique de sécurisation du logiciel aussi bien dans son exécution que dans sa spécification. Pour exemple, T.J. Tanzi et C. André [TANZI 1999] on choisi pour la modélisation des mouvements des patrouilleurs de l'autoroute A8. Leur étude portait sur la sécurisation des échanges d'informations entre les différents utilisateurs et le poste de commande. En effet, les échanges d'information entre le terrain et le poste central s'effectuent essentiellement avec le réseau d'appel d'urgence. Or, le positionnement des patrouilleurs utilisant aussi ce réseau il était nécessaire de démontrer que les spécifications initiales étaient respectées, en particulier, dans les différentes configurations de partage d'une même ressource. En considérant, le système comme un ensemble d'agents interagissant, le comportement de chacun a été décrit à partir d'une représentation graphique SYNCCHARTS directement traduit en langage ESTEREL. Ils ont ainsi pu modéliser le comportement des différents acteurs et décrire les différents échanges comme des signaux. Le modèle obtenu permettait de simuler le comportement du système à partir du comportement des agents, ce, afin de pouvoir jouer tous les scénarii possibles de comportement de ces agents mais aussi de défaillances du réseau. L'intérêt essentiel de la démarche a été de pouvoir s'intéresser à la modélisation d'un système complexe en s'appuyant sur un modèle réactif sans avoir à prendre en compte le comportement intrinsèque du logiciel et en présentant à l'utilisateur une interface graphique compréhensible et informative.

La réduction du risque en phase d'exploitation

La phase projet qui intègre spécification, conception et réalisation du système est organisée autour d'objectifs clairs et communs de coûts et de délais. Même si le processus de gestion des risques apparaît relativement indépendant, il ne se différencie du reste du projet que par ses objectifs fonctionnels.

La phase projet est une phase logique qui anticipe le fonctionnement et l'exploitation du système sur la base des connaissances disponibles, par des calculs et des dispositions organisationnelles. Pendant cette phase sont définies des conditions de fonctionnement normales ou dégradés, ainsi que les modes de réponse générique à des situations exceptionnelles types.

La phase de spécification établit les prescriptions constructives à partir de prévisions. Il reste nécessaire pour l'exploitation d'assurer le récolement entre d'une part, les prescriptions provenant des différentes entités qui ont conçu le système et construit les installations, et d'autre part, la réalité du fonctionnement effectif des équipements et des installations et du comportement des acteurs (opérateurs et utilisateurs).

Ainsi, au terme de la phase de projet et avant la mise en service des installations, les procédures d'exploitation, d'entretien et d'inspection sont définies à partir de l'expression d'exigences des différents concepteurs et constructeurs.

Ces consignes et procédures ont donc par essence une dimension technique et rationnelle et cantonnent la future réalité dans la prévision. Sauf à tenter de décrire dans les plus intimes détails

tous les états envisageables d'un système, ces consignes et procédures ne peuvent offrir qu'un cadre a priori "vrai" mais inéluctablement réducteur et simplificateur de la réalité.

L'écart existant entre la prescription et la réalité résulte de l'impossibilité d'enfermer dans une prévision totale l'ensemble des situations susceptibles d'être rencontrées dans l'exploitation d'un système dont la complexité résulte des aspects : techniques, organisationnels et humains.

Le retour d'expérience.

Une réponse à cette problématique peut être la démarche de "retour d'expérience" qui consiste à se mettre "à l'écoute des signaux provenant de l'installation" et à se saisir de tout accident, incident, anomalie pour en retirer le maximum d'enseignements. Le retour d'expérience revêt ainsi deux aspects :

- d'une part, d'un élément de compréhension et d'accroissement des connaissances,
- d'autre part, d'un élément essentiel de toute démarche managériale par l'implication des acteurs et la recherche de progrès.

La démarche de retour d'expérience traite les événements sortant du cadre prescrit pour en rechercher les causes et définir les actions correctives. Cette démarche agit en réaction aux événements constatés sur les installations dans les différentes phases d'exploitation. C'est une démarche a posteriori qui a pour objet de traiter systématiquement tout événement détecté en dehors des conditions nominales. La démarche de retour d'expérience permet d'enrichir la connaissance du comportement du système, et, prolonge d'une certaine manière la phase de projet. Cette démarche trouve son efficacité dans l'organisation mise en place pour détecter les événements, d'où la nécessité d'impliquer l'ensemble des acteurs lutte contre la perte d'une vision globale des objectifs de sécurité ou contre l'oubli de la justification des mesures.

Dans le transport il est de règle d'analyser, par des procédures adaptées, toute anomalie, tout incident ou accident pour en rechercher les causes et leurs enchaînements, et tirer les enseignements. L'approfondissement de l'analyse dépend de la complexité des situations et de la gravité potentielle ou avérée des conséquences. L'analyse pour les événements complexes et sérieux s'effectue en plusieurs étapes :

- une analyse immédiate permettant d'avoir une première idée des circonstances et des conséquences, d'adopter des premières mesures et de fournir un premier niveau d'information,
- une analyse technique ayant pour objet d'identifier les éléments techniques du déclenchement des événements, de leur déroulement et de leurs conséquences,
- une analyse détaillée complétant l'analyse technique sur tous les autres aspects relevant des domaines de l'organisation, des procédures, de la formation et du comportement.

Il s'agit d'un processus long et détaillé, encadré par l'administration et les différentes autorités. Afin d'améliorer la démarche de maîtrise des risques, il est de pratique courante de compléter la démarche de retour d'expérience par une démarche pour détecter et analyser les conditions ou les actions porteuses de risques.

A contrario de la démarche de maîtrise des risques en phase projet qui est une démarche plus technique confiée à une équipe dédiée, la démarche de retour d'expérience est une démarche participative impliquant l'ensemble de la structure d'exploitation. La mise en commun d'objectifs, la vision système qu'implique le dialogue et la mobilisation de corps techniques différents dans le partage des connaissances et des expériences font de cette démarche un pont entre l'approche système et l'approche systémique.

La défense en profondeur

La notion de base qui définit le concept de défense en profondeur est que tous les éléments sont considérés comme émettant des flux auxquels d'autres éléments sont sensibles. Le flux généré devient alors un danger et le risque est qualifié par la probabilité que le flux atteigne l'élément sensible. Face à l'impossibilité de neutraliser l'élément source ou de désensibiliser l'élément cible il devient donc nécessaire d'interposer des barrières pour stopper, dévier ou transformer le flux de danger.

Le concept de défense en profondeur est un concept fondamental de la sécurité nucléaire qui considère que malgré l'ensemble des méthodes et des techniques employées en ingénierie du risque, la probabilité d'accident continue d'exister. Compte tenu de cet état de fait, il devient alors nécessaire d'examiner les dispositions de conception ou d'exploitation propres à en limiter les conséquences à des niveaux estimés acceptables. Ainsi pour répondre au risque principal qui est la dissémination de substances radioactives sont interposées des barrières entre les personnes et les substances. La défense en profondeur consiste donc à réduire le risque technologique sur les barrières :

- en empêchant une sortie du domaine de fonctionnement de l'installation,
- en maîtrisant les écarts par rapport à un fonctionnement normal,
- par la mise en place de systèmes dits de sauvegarde pour limiter les conséquences d'un dysfonctionnement sur les barrières,
- par la mise en place de dispositions visant à limiter les conséquences de défaillances multiples et à renforcer la barrière ultime
- par la mise en place de plans et de dispositions internes aux installations et externes (plans d'urgence et plans d'interventions des pouvoirs publics) pour assurer la protection ultime des populations.

Le concept de défense en profondeur correspond ici à une stratégie déployée face à un objectif déterminé et conduite à différents niveaux de conséquence d'un accident afin d'en réduire la gravité.

Afin de requalifier et d'évaluer l'ensemble de ses mesures de protection contre les accidents, la RATP a mis en place un formalisme de représentation des barrières. Ce formalisme permet de représenter les différentes situations face au comportement de la barrière et d'évaluer ainsi l'efficacité d'une défense; il permet aussi de définir les exigences de conception, maintenance et d'utilisation des barrières en fonctions des évolutions des systèmes agresseurs et agressés.

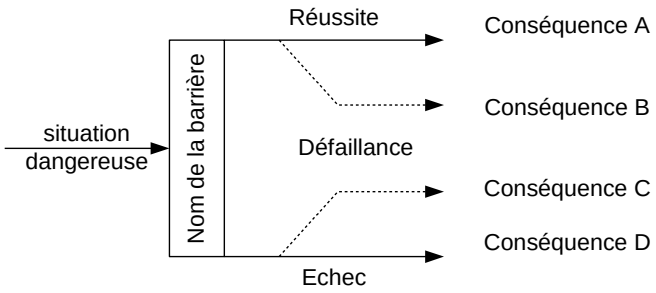


Figure 16 : Formalisme de représentation d'une barrière pour la défense en profondeur à la RATP

La dualité sécurité - fiabilité

Enfin, pour terminer cette large présentation de l'ingénierie du risque il est intéressant de noter que les analyses de sécurité et de fiabilité utilisent souvent les mêmes valeurs de seuil, et que les méthodes par lesquelles les démonstrations de sécurité ou de fiabilité se construisent sont analogues. L'illustration de ce rapprochement apparaît dans le regroupement des textes normatifs relatifs à ces activités sous un même référentiel méthodologique et un regroupement des activités sous la terminologie FMDS[1] ou RAMS[2] en anglais. Ces deux critères restent toutefois très différents dans leurs objectifs :

Fiabilité	**Sécurité**
S'applique le plus souvent à un équipement ou un matériel considéré.	S'applique nécessairement à un système et met l'accent sur les problèmes d'interaction.
Ne prend généralement pas en compte les facteurs humains.	Considère l'homme comme un élément du système étudié.
Etudie le bon fonctionnement d'un matériel dans des conditions d'utilisation bien spécifiées.	Doit envisager toute circonstance, normale ou anormale, pouvant conduire à une situation dangereuse.
S'intéresse à des évènements dont le coût est du même ordre de grandeur que celui du coût normal d'une mission.	S'intéresse à des évènements dont le coût est d'un ordre de grandeur nettement supérieur à celui du coût normal d'une mission.
S'attache à des évènements qui peuvent être généralement appréhendés par l'expérience et le traitement statistique.	S'attache à de multiples combinaisons d'évènements, dont chacune peu probable, échappe à une exploitation statistique simple.
Peut entrer en conflit avec la sécurité et exiger parfois des solutions techniques différentes.	Peut être améliorée par de multiples moyens, l'augmentation de la fiabilité de certains éléments n'étant qu'un de ces moyens.
Font appel au calcul des probabilités et aux méthodes de la statistique.	
Se construisent par des moyens comparables (application de spécifications, existence d'un véritable plan de qualité, revues de projets, recueil et traitement d'information techniques…).	
Plan de fiabilité et programme de sécurité s'étendent sur toute la vie du système ou du matériel, depuis la conception jusqu'à la mise au rebut.	

[1] FMDS : Fiabilité, Maintenabilité, Disponibilité et Sécurité

[2] RAMS : Reliability, Availability, Maintenability, Safety

L'APPROCHE SYSTEME : LA GESTION DU RISQUE

La maîtrise des risques

Les discours entendus dénotent souvent d'une confusion entre l'analyse des risques et la maîtrise des risques. Il y a pourtant une différence essentielle entre ces deux activités. L'analyse des risques est un domaine d'activité pour lequel la motivation principale est la recherche, alors que la maîtrise des risques a pour objectif de gérer le risque pour le maîtriser. L'analyse des risques est donc une activité tactique, alors que la gestion des risques est une activité stratégique. La nécessité d'avoir à identifier et à évaluer le risque avant de le maîtriser conduit à la confusion des genres; de même qu'on confond souvent tactique et stratégie. Il faut considérer que l'analyse et la gestion des risques sont les deux processus essentiels répondant à une volonté qui est la maîtrise des risques. La Maîtrise des Risques est une activité de décisions, motivées par des objectifs. Ce sont ces objectifs qui déterminent les moyens et les stratégies. La Maîtrise des Risques est un système opérationnel. L'analyse des risques est le processus de détection des éléments caractéristiques du risque. Ce processus peut être conduit suivant différentes méthodes répondant à un objectif unique, détecter les éléments correspondant à une situation de danger. La gestion des risques est l'outil de traitement de l'information générée par l'analyse.

La Maîtrise des Risques est un système défensif qui par le nombre réduit et la simplicité de ses objectifs, s'apparente à un système de défense militaire. En effet, nous retrouvons les trois principales activités d'un système de combat : détection, évaluation de la menace (classification) et décision. De même que dans tout système équivalent, des seuils sont déterminés de façon à filtrer les informations en sortie de l'analyse

La Maîtrise des Risques repose sur un équilibre judicieux entre la satisfaction des objectifs du système et l'acceptation du risque encouru dans sa mise en œuvre. C'est une activité relevant d'un système de décision complexe (choix des finalités et des moyens de les satisfaire), qui est déterminé par le gestionnaire des risques de façon autonome ou solidaire à l'organisation dont il est membre. Il existe deux politiques dans le management des risques :

- la politique du systématique qui est applicable dans les milieux scientifiques ou l'industrie à haut risque,
- une démarche allégée utilisant beaucoup les principes du GAME dont les analyses souvent empiriques aboutissent parfois à une couverture des risques abandonnée à la régulation.

Il faut noter que le principe du GAME, globalement au moins équivalent, ne s'appuie pas sur une analyse mais sur le retour d'expérience; en effet, ce principe admet qu'un retour d'expérience suffisant permet de lever (et non de couvrir) un risque potentiel.

Cependant ces deux politiques ne constituent pas les différences essentielles entre les techniques et méthodes de la maîtrise des risques, elles sont simplement révélatrices des moyens disponibles ou consentis pour gérer les risques d'un système. Les différences essentielles entres les approches dépendent surtout de ce qu'elles s'intéressent au composants du système ou au système dans sa globalité.

D'après C. Lievens [LIEVENS 1976] l'intérêt de l'approche système est que dans l'approche classique la réduction de la complexité par décomposition en éléments simples suppose que les interactions entre les éléments sont nulles. Cette définition revient à ramener la notion de système à un ensemble technique. Or, un système est un ensemble organisé et articulé dont les éléments fonctionnent en synergie pour accomplir une ou plusieurs missions et dont le niveau de complexité technique est d'un ordre de grandeur nettement supérieur à celui de chacun des

constituants. Néanmoins, la réunion de sous systèmes optimaux ne constitue pas un système optimal (Théorème de Bellman qui décrit surtout le principe d'optimalité : « une suite de décision optimale n'entraîne pas globalement une décision optimale »). Ceci est d'autant plus vrai et critique lorsque l'intégrité de la sécurité peut être remise en cause.

Le processus de maîtrise des risques relève d'une approche systématique et documentée basée sur la démonstration que l'ensemble des risques engendrés par le système et par ses ensembles techniques ont été identifiés, évalués et couverts par des foncions de sécurité. Cette démarche est assurée par des concepts d'ingénierie, des méthodes, des outils et des techniques reconnus et appliqués tout au long du cycle de vie du système. Ce processus est souvent confondu avec la démarche dite de FMD (Fiabilité, Maintenabilité et Disponibilité) car les méthodes et outils sont identiques et la sécurité et la disponibilité sont interdépendantes. En effet, une mauvaise gestion des conflits entre leurs exigences propres peut s'opposer à l'obtention d'un système sûr, ou a contrario à l'obtention d'un système tellement sûr qu'il n'est jamais disponible. De plus, les objectifs de sécurité et de disponibilité ne peuvent être atteints qu'en satisfaisant aux exigences de fiabilité et de maintenabilité du système et en contrôlant dans la durée de manière permanente les activités de maintenance, d'exploitation ainsi que l'environnement du système.

Si nous reprenons la définition de la norme MIL-STD-882 [MIL 2002] : "la sécurité d'un système est égale au degré de sécurité optimale compatible avec les contraintes d'efficacité opérationnelle, les coûts et les délais, et qui doit être obtenu par application systématique des principes de sécurité (conception et conduite) au cours des phases successives de la vie du système". Cette définition implique :

- la détermination d'un objectif de sécurité à partir d'une étude d'optimisation coût - efficacité - délai,
- des méthodes rigoureuses de la conception à l'utilisation.

Le processus de maîtrise des risques s'appuie sur la mise en place d'un programme sécurité débutant en phase de définition système et se poursuivant tout au long du développement du système. Ce processus de construction de la sécurité est itératif (analyse, édition de critères, validation) et permet de garantir que la sécurité et son maintien en opération, se traduit par la mise en place d'actions. Ces actions permettent de classifier les risques et d'en identifier les causes puis de définir les principes de mise en sécurité. Ces principes de sécurité son ensuite traduits en critères qui appliqués garantissent l'atteinte des objectifs de sécurité fixés ou qu'au moins les scenarii résiduels restent compatibles avec ces objectifs. Par scenarii résiduels il faut comprendre toutes les combinaisons conduisant à une situation redoutée pour lesquelles aucune parade technique n'a été trouvée.

Pour des systèmes à niveau d'intégrité de la sécurité élevé, et pour éviter les conflits d'objectifs entre respect d'un budget coûts – délais, et respect d'in objectif de sécurité, ce processus est normalement conduit par une équipe indépendante du développement du système qui effectue l'ensemble des analyses de risques et de défaillances et qui réalise l'ensemble des vérifications permettant de vérifier la couverture des exigences de sécurité. Pour les systèmes de transports urbains guidés, le travail de cette équipe est lui-même évalué par un "second regard" indépendant qui valide les aspects méthodologiques et de couverture dans le processus de maîtrise des risques.

L'ingénierie du risque : un processus parallèle

L'ingénierie du risque est une véritable activité avec un objectif, une méthodologie et des outils adaptés. L'ensemble des normes relatives à la sécurité des systèmes définit la démonstration de la sécurité comme une démarche cohérente de gestion de la sécurité qui intervient depuis la spécification des besoins d'un système jusqu'à son retrait du service. Pourtant la difficulté

principale réside dans le fait que les travaux de l'ingénierie du risque sont effectués en co-activité avec le développement ou l'exploitation du système. Il est donc nécessaire que le phasage et les objectifs intermédiaires des deux activités fonctionnent sur un schéma commun, ce schéma commun est le cycle de vie du système.

Déterminer l'origine du danger revient à identifier ce que l'on cherche. En effet, la perception du danger est surtout liée à la connaissance que nous avons de certaines conséquences et des situations qui y conduisent. Les analyses de risques utilisent la connaissance générale ou retour d'expérience pour identifier les cas de danger. Le principe consiste donc à affiner la connaissance du système analysé pour détecter les conditions pouvant conduire à des situations connues par avance. Le processus a la même nature qu'un filtre et comme tout filtre il déforme l'objet observé en en fournissant une image réductrice.

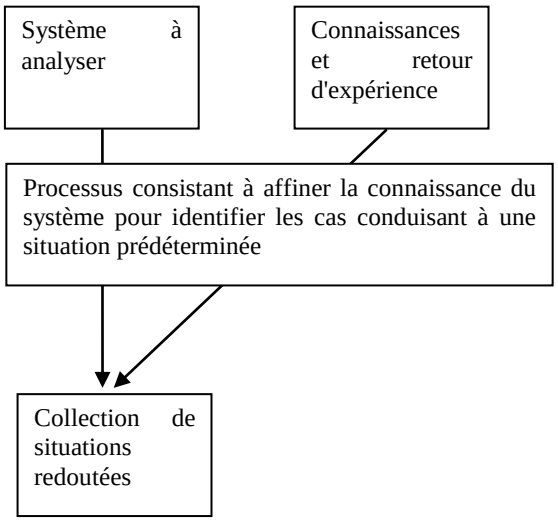


Figure 17 : Processus global d'identification de situations redoutées

Le danger fait partie intégrante du système, sa détection ou visibilité relève plus de l'acuité de l'observateur, autrement dit de sa capacité à observer le système. Le fait de signaliser certains évènements ou d'identifier des précurseurs de dangers sont une parfaite illustration de l'impact des connaissances sur le système. La détection du danger ne peut se faire qu'à partir :

- de la reconnaissance de certains signaux,
- de la reconnaissance de certains objets
- de la reconnaissance de certaines relations.

Dans ce cas, l'analyse cherche à épuiser le modèle en explorant toutes les combinaisons, soit cherche à reconnaître les signaux. Se retrouvent là les principes de management des risques : la connaissance des dangers puis la connaissance du système observé, ou, l'observation d'un système donné à travers son propre système de connaissance. Ce processus :

- fourni une vision orientée du système,
- requiert une exhaustivité de la collection obtenue,
- implique un processus itératif du système modifié jusqu'à épuisement des cas sources de situations dangereuses,
- surtout, implique un système défini, bordé et stable.

Etant donné que la conception d'un système a pour vocation de fournir certains services, l'analyse des risques ne peut être qu'une démarche complémentaire et itérative d'étude du système.

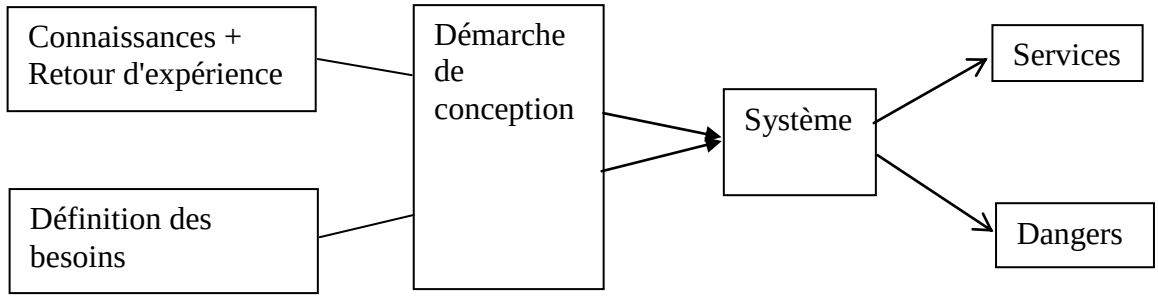


Figure 18 : Processus de conception et dangers

Les dangers sont alors un sous produit du système, ils sont simplement indésirables, d'où l'intérêt d'un modèle pour tenter d'anticiper leur occurrence. Cependant comme le danger est par nature inconnu et inattendu (ou plutôt on espère son absence) il serait donc impossible a priori de le décrire avec le même processus que la modélisation du fonctionnement système d'où l'obligation d'itération du processus.

Les méthodologies choisies ont alors pour vocation de faire converger rapidement les deux démarches sans pour autant les dégrader.

Le cycle de vie du système

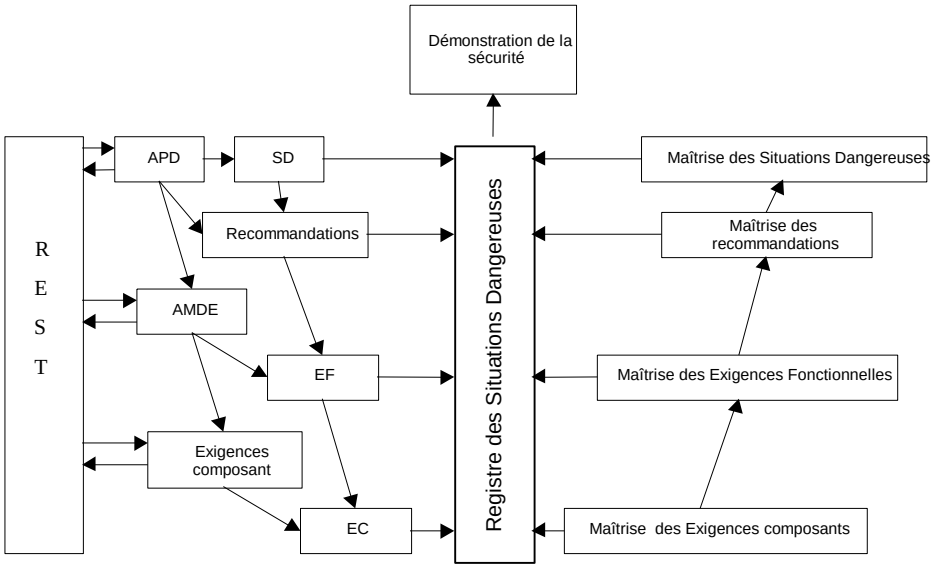
L'intérêt de la définition d'un cycle de vie est qu'il fournit un cadre pour la programmation, le management, le contrôle et la surveillance du système sous tous ses aspects, en particulier la sécurité, en définissant une succession de phases ainsi que les tâches relatives à chaque phase et à la transition entre chaque phase.

L'objectif lié à l'application de ce processus méthodologique est d'obtenir la collaboration entre les activités générales du projet et les activités relatives à la sécurité afin d'établir un équilibre entre les performances de sécurité du système et les contraintes de développement (coûts, délais, complexité…).

Le processus de démonstration de la sécurité

Une rapide analyse des tâches décrites dans ce tableau montre que le processus est essentiellement documentaire, c'est-à-dire que la démonstration de sécurité se construit par la documentation de preuves soit de vérification soit de conformité. Ce point est justifié par le fait que le processus est itératif, c'est-à-dire que la démarche est reconduite et précisée à chaque phase du cycle de vie. On verra par la suite que l'application de simples parades technologiques est insuffisante pour garantir la sécurité globale d'un système.

En dehors du fait que le processus est élargi à la notion de système, celui-ci est toujours articulé autour des phases de définition des objectifs, d'identification des risques, d'allocation des objectifs de sécurité, et de couverture de ces risques.



APD : Analyse Préliminaire des Dangers
AMDE : Analyse des Modes de Défaillance
SD : Situations Dangereuses
EF :Exigences Fonctionnelles
EC : Exigences Composants
REST : Recueil des Exigences Sécurité sur le Système tramway

Figure 19 : Processus de maîtrise des risques

L'analyse des risques

Dans les méthodologies de maîtrise des risques, l'analyse des risques est le processus qui va permettre l'allocation des niveaux d'intégrité de la sécurité aux différentes fonctions des équipements, des sous systèmes et du système. Ce processus passe par une démarche systématique et l'application des outils abordés précédemment (§ 0) prenant en compte à la fois l'environnement du système et son modèle architectural. Le résultat est une liste de situations dangereuses et de taux maximum d'occurrence de danger.

L'analyse de risque doit être effectuée à diverses phases du cycle de vie du système. Pour être complète celle-ci ne doit pas se contenter de la production d'une liste plus ou moins exhaustive de situations dangereuses mais être bâtie sur une méthodologie qui identifie clairement les hypothèses, les limites et les justifications de l'étude. L'étude doit fournir une justification des estimations de risques à partir des données connues (en fonction de la pertinence et du niveau de confiance de leurs sources) en recherchant un compromis entre la recherche d'un état sûr à tout prix et les contraintes de disponibilité ou de coût du système.

La parade méthodologique

L'application des méthodes de conception et de réalisation en sécurité va donc conduire à un comportement déterministe de l'équipement, dont un des états sera considéré comme l'état de sécurité. En ferroviaire, une défaillance va se traduire par l'arrêt du train ou par le maintien fermé d'une barrière de passage à niveau. Il faut tout de même considérer l'aspect système de la sécurité

ferroviaire, car il y a une certaine corrélation entre le nombre d'arrêts intempestifs de trains et le nombre de collisions. En effet, l'arrêt intempestif de trains devant un signal fermé a pour effet de condenser ceux-ci sur la ligne et d'augmenter la probabilité de rattrapage. De plus, l'impossibilité de maintenir les trains à l'arrêt en ligne jusqu'à réparation implique la mise en œuvre d'une procédure spéciale pour leur remise en route, ce qui augmente le risque. De même, la fermeture prolongée sans passage de train d'une barrière de passage à niveau conduit les usagers de la route à passer à leur seule initiative et augmente considérablement le risque de collision.

Le processus de maîtrise des risques s'appuie sur la mise en place d'un programme de sécurité débutant en phase de définition système et se poursuivant tout au long du développement du système et de ses constituants. Comme il a été dit précédemment, ce processus de construction de la sécurité est itératif (analyse, édition de critères, validation) et permet de garantir que la sécurité et son maintien en opération, se traduit par la mise en place d'actions afin de :

- répertorier et de classifier les risques et d'en identifier les causes,
- définir les principes de mise en sécurité au niveau fonctionnel et au niveau des moyens et des techniques associés,
- gérer la mise en application de ces critères, de vérifier leur prise en compte et d'identifier les points sécurité ouverts,
- valider la conception en vérifiant l'obtention des critères par une analyse des solutions techniques.

Cette validation permet aussi de démontrer le respect des objectifs de sécurité, en particulier les scénarii résiduels devant être compatibles avec les objectifs définis par les obligations vis-à-vis de la sécurité.

Le dossier de sécurité, document unique comme preuve de la sécurité

Le dossier de sécurité est l'élément essentiel dans la démonstration de la sécurité d'un système par l'application de ces deux principes. Ce document apporte la démonstration que la preuve de la sécurité d'un système a été faite par une approche systématique et documentée, basée sur des preuves qualitatives (assurance qualité ou assurance sécurité), des preuves techniques ou des preuves de contrôle par un regard extérieur. Il n'est pas nécessaire d'inclure beaucoup de preuves et de documents détaillés dans le dossier de sécurité et ses différentes parties, pourvu que les références précises soient données à de tels documents et que les concepts de base et les démarches utilisées soient clairement spécifiés.

Gestion de la qualité

La preuve de la gestion de la qualité doit démontrer qu'un système de gestion de la qualité efficace tout au long du cycle de vie du composant, sous système ou système a été mis en place. L'objectif de ce système qualité est de minimiser l'incidence de l'erreur humaine à chaque phase du cycle de vie. Parmi ces points qui doivent être couverts par le système qualité on trouve :

- La structure et l'organisation,
- Le planning et les procédures qualité,
- Le traitement des non conformités et des actions correctives,
- La gestion de configuration et le contrôle des évolutions.

Gestion de la sécurité

La preuve de la gestion de la sécurité doit démontrer qu'un système de gestion de la sécurité efficace tout au long du cycle de vie du composant a été mis en place. De la même façon, l'objectif de ce processus est de minimiser l'incidence de l'erreur humaine. Le processus de gestion de la sécurité s'appuie sur une organisation et une documentation spécifique.telle qu'un

plan d'assurance sécurité, lequel identifie la structure et les activités et les points d'approbation et un registre des situations dangereuses, répertoriant les situations dangereuses identifiées.

Démonstration de la sécurité fonctionnelle et technique

La démonstration de la sécurité fonctionnelle et technique est apportée par un rapport qui doit expliquer les principes techniques garantissant la sécurité de la conception, incluant toutes les preuves de soutien : principes de conception et calculs, spécifications et résultats d'essais, analyses de sécurité. Lorsque les niveaux de sécurité ont été fixés, et que les critères de réduction des risques ont été déterminés, il est possible de décliner les exigences de sécurité sur les fonctions, composants, sous-systèmes et système.

LES APPROCHES SYSTEMIQUES

Système, complexité et systémique

Quelque soit les méthodes employées et leur niveau de sophistication, les analyses de sécurité répondent toujours aux mêmes principes fondamentaux. L'analyse classique des modes de défaillance construit un arbre à partir de la structure organique d'un système en analysant les probabilités de défaillance. Or, ces analyses ne conduisent qu'à s'intéresser aux chemins structurels du système, les aspects environnements global et interaction doivent être traités par une approche plus globale. On a pu constater dans les chapitres précédents que cette approche globale est définie par un cadre méthodologique. Lorsque le système a un comportement plus complexe et qu'il prend en compte non plus des objets technologiques mais des comportements évolutifs, il devient intéressant d'analyser le système différemment : on utilise alors les approches systémiques.

La systémique se définit comme une approche modélisatrice de phénomènes complexes. En d'autres termes lorsque nous admettons avoir un système nous avons déterminé un objet avec ses limites; or, là intervient la notion de complexité. Pour reprendre E. Morin [MORIN 2002], "la complexité étant un problème complexe, c'est compliqué de l'exposer". E. Morin introduit ainsi son article "à propos de la complexité", ceci pour expliquer que derrière cette notion nous tentons souvent de cacher une forme d'incapacité à appréhender la chose dite complexe ; incapacité ne veut par dire refus ou renoncement à décrire ou comprendre.

Dans la représentation que nous faisons d'un système à travers des événements subis ou générés, nous commençons par évaluer la variété des comportements possibles de celui-ci. Si les facteurs restent peu nombreux (nombre d'entités, nombre d'actions réalisables…) nous admettons rester en présence d'un système simple. Par contre, si le système présente un nombre élevé d'associations, de combinaisons ou de relations nous considérons être face à un système complexe; ceci, uniquement car il est non entièrement appréhendable. Remarquons que nous collons ici à la racine étymologique latine "complexus", ce qui est tissé ensemble. Nous voyons le motif, mais nous ne discernons pas le détail du fil. Complexe n'a rien à voir avec compliqué; notre incapacité à appréhender à la fois le motif et le détail du fil n'implique pas que celui-ci ne soit pas d'une structure simple.

Ainsi l'approche système va donc observer la chose telle qu'elle est sur un domaine d'évolution connu. Les techniques étant déterminées celle-ci relèvent alors du domaine de l'ingénierie. L'approche systémique va tenter d'appréhender une chose perçue complexe, dont par définition on ne possède pas les clés pour sa compréhension (connaissances ou techniques appropriées). Comme toute approche nécessite tout de même un minimum de méthode, la systémique fonde sa démarche sur le concept de système et sur le concept associé de modèle. La notion de système est et reste la notion de base pour désigner tout ensemble de relations entre constituants formant un tout. Le modèle est construit pour appréhender le système et son comportement. L'approche systémique fournit les principes méthodologies et langages, permettant de coordonner les différents points de vue (métiers, sciences, cultures, organisation) sous lesquels est abordé le système observé.

Enfin on ne peut parler d'approche systémique sans aborder le paradigme systémique tel que l'a fait émerger J.L. Le Moigne [LE MOIGNE 1977] dans son ouvrage intitulé "Théorie du système général : théorie de la modélisation". L'auteur y décrit cinq concepts se trouvant implicitement ou explicitement dans la notion de système : activité, structure, évolution, finalité et environnement. Cette construction théorique, artificielle est baptisée système général. Le concept

fondamental de la modélisation systémique n'est pas l'objet, ou la combinaison d'objets stables (structure) mais l'action. La caractérisation de l'action passe par la notion générale de processus. Un processus peut être défini comme l'ensemble ordonné des changements qui affectent la position dans le temps, dans l'espace, dans la forme ou dans la nature, d'une famille d'objets identifiés. Le concept de processus évoque toujours une dualité objets processés/objets processeurs et une description des changements affectant les objets processés.

Tout modèle d'un objet dans son environnement ou tout modèle de son comportement peut être conceptualisé par un processus. Le processus représentant une transaction à un instant donné entre deux objets, dont le premier est l'intrant et le second l'extrant. La relation du système avec l'environnement est caractérisée par deux phénomènes :

- une transaction (ou échange) du système avec l'environnement.
- une capacité d'influence de l'environnement sur le système.

L'approche systémique a produit un modèle descriptif de représentation d'un système : tout système peut être découpé en trois sous systèmes : un sous-système opérant, un sous-système d'information et un sous-système de pilotage. Enfin l'approche systémique se voulant d'abord une approche de réduction de la complexité, la démarche permet de représenter le réel comme l'emboîtement de systèmes. La démarche est donc une approche du général au particulier.

L'approche systémique n'est pas une approche nouvelle. Celle-ci est apparue au siècle des lumières et était plutôt orientée "objets". Une deuxième forme d'approche axée sur le vivant est apparue avec la biologie du vingtième siècle. Enfin, aujourd'hui une troisième génération d'approche systémique, apparue vers 1970 est tournée vers les systèmes sociaux (équipes, entreprises…). Nous retrouvons là le schéma des évolutions des démarches sécurité : dans un premier temps l'objet est en cause, puis son comportement et enfin la totalité de la structure utilisatrice. D'un point de vue plus global l'intérêt de l'approche systémique est que dans ce contexte de pensée, un système peut être défini de la façon la plus générale comme un tout organisé de composants en interaction. Cette définition très générale met en évidence les trois catégories d'entités nécessaires pour décrire un système générique: les objets (composants), les réseaux de relations (interactions) et la globalité du système (entité existante au sein d'un monde plus vaste). L'approche systémique actuelle s'intéresse non seulement au relations et comportements dans le système mais aux influences que celui-ci peut avoir subir vis à vis du monde dans lequel il évolue.

En utilisant un raccourci très simplificateur et critiquable, on peut poser que l'approche système s'intéressera à un réseau de relations organisé au sein d'un ensemble cohérent, homogène et isolé, alors que l'approche systémique considère le système comme un tout non-isolé capable d'échanger et va donc s'intéresser aux flux pas toujours cohérents générant des situations et des comportements complexes et évolutifs.

Les méthodologies systémiques

MADS - MOSAR

MADS (Méthode d'Analyse des Dysfonctionnement dans les Systèmes) a été initiée par l'Université de Bordeaux I. Les auteurs des cette approche appellent science du danger le corps de connaissance qui a pour objet d'appréhender des évènements non souhaités (ENS).

Le principe de modélisation des processus de danger est celui du modèle Source-Cible-Flux-Champ. Le principe en est que le domaine est décrit par l'ensemble des processus qui s'y déroulent. Tout processus émet des flux. La notion de flux est indissociable de la notion complémentaire de champ, le flux participant au processus actif, et le champ à l'environnement actif. Le champ est vu comme "une capacité d'influence": c'est l'ensemble des éléments qui influent sur le processus sans en faire partie (le vent sur un incendie, le stress dans une erreur humaine). Le flux, dans un processus est vu comme un chemin de transfert entre deux processus. Il relie donc deux sous-systèmes, appelé source et cible, qui caractérisent le processus au même titre que le flux et le champ. L'ensemble pouvant se représenter schématiquement ainsi :

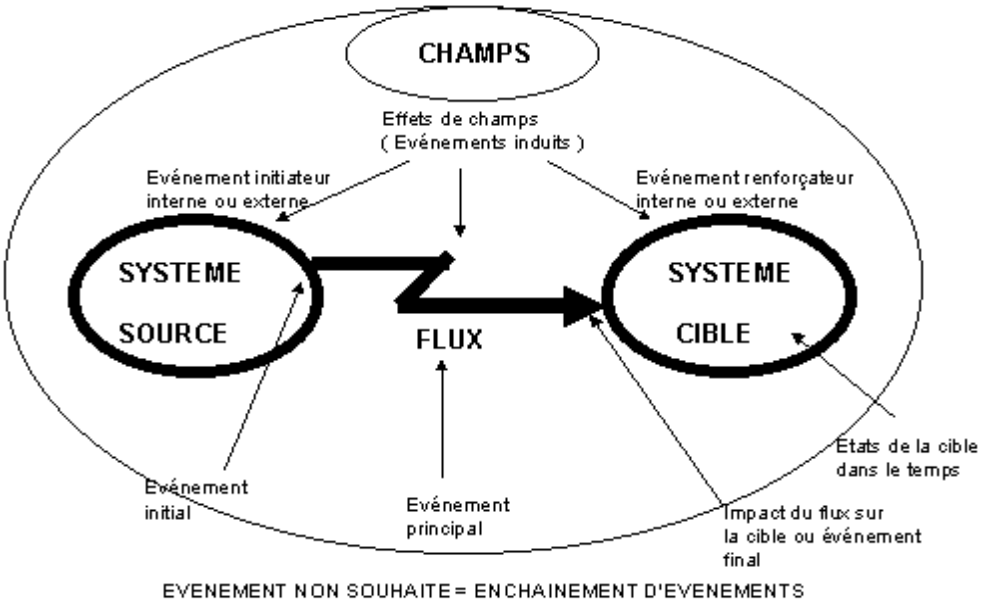


Figure 20 : Modèle MADS [PERILHON 1999]

Les flux sont essentiellement des flux de matière, d'énergie ou d'information mais la typologie peut être étendue par exemple aux flux cognitifs. Les processus de source ou de cible sont des processus de forme (transforme le flux) ou de nature (transmute le flux), les processus de champs sont des processus de temps ou d'espace.

La modélisation MADS est une modélisation systémique qui permet une représentation de processus de danger macroscopiques et microscopiques.La méthodologie associée de production des modèles de danger se décline en trois étapes :

- l'identification et la représentation générale des systèmes sources et cibles,
- puis représentation des systèmes sources de danger et des systèmes potentiellement cibles,
- enfin, la modélisation des processus de danger avec la représentation des champs de danger.

La mise en œuvre opérationnelle de la méthode MADS a été formalisée dans la méthode MOSAR ou Méthode Organisée et Systémique d'Analyse de Risque. MOSAR est une méthode permettant de structurer une démarche d'analyses des risques technologiques élaborée dans les années 70 par P. Périlhon [PERILHON 2003]. La méthode a recours aux mêmes types d'outils que les AMDEC, HAZOP, etc.

La méthode se décline en deux modules appelés simplement module A et module B. Le module A permet de réaliser globalement sur le système, une analyse des risques principaux à partir d'une décomposition en sous systèmes. Le module B sert à analyser plus finement le système en détaillant les risques à partir des outils de la sûreté de fonctionnement. La représentation schématique suivante résume les différentes étapes de la méthode MOSAR.

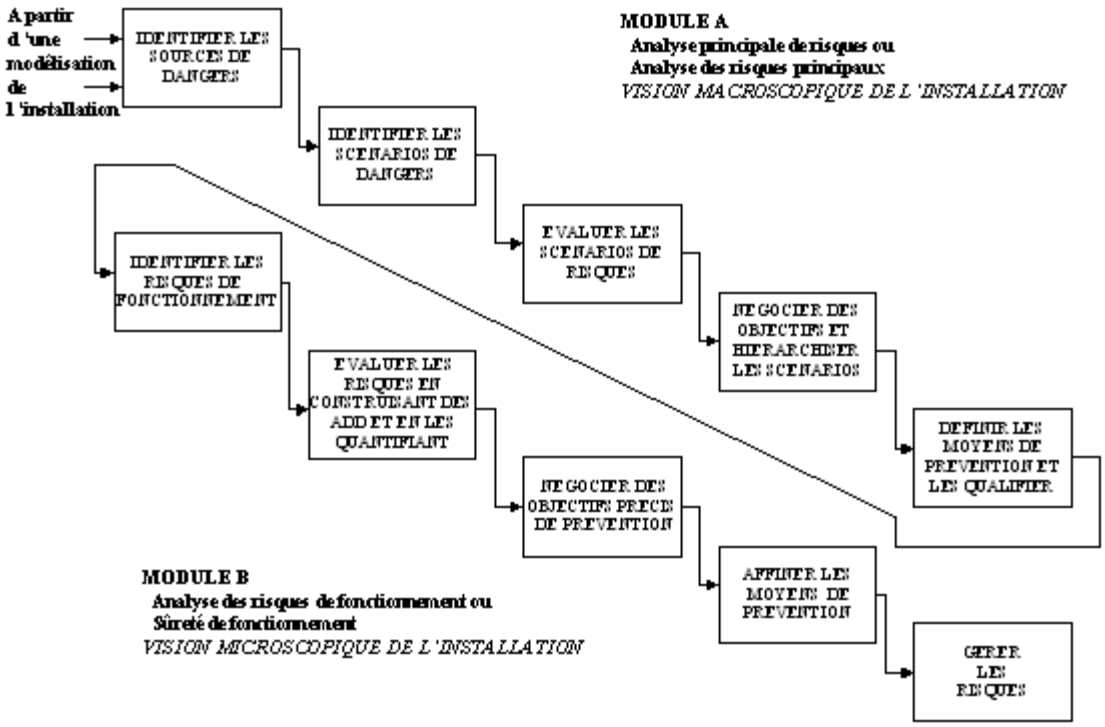


Figure 21 : Structure de la méthode MOSAR [PERILHON 2003]

SAGACE

La méthode SAGACE est une méthode systémique qui a été développée par Mr Penalva au CEA pour la modélisation du rôle de l'opérateur dans la conduite de processus complexes. La méthode est utilisable en conception, exploitation ou pour l'amélioration de systèmes techniques, organisationnels ou stratégiques. Le développement de la méthode SAGACE part de l'importance majeure qu'a la structuration dans la représentation système et propose un modèle intégrant les différentes décompositions du système. Le modèle proposé réduit ainsi la complexité de la représentation d'un système en modélisant les processus selon différents points de vue. Pour déterminer les points de vue le système évalué suivant trois axes de perception ou vision :

- La vision fonctionnelle, ce que fait le système,
- La vision organique, ce qu'est le système,
- La vision stratégique, ce que décide le système.

Chaque axe de perception du système est analysé selon trois niveaux correspondant chacun à une perception de la dynamique du système. Les activités, le fonctionnement et l'évolution. Le système est alors décrit suivant chaque point de vue :

- fonctionnel – activité : par des modèles d'architecture fonctionnelle (SADT…) des diagrammes de flux…
- fonctionnel – fonctionnement et fonctionnel-évolution : par des scénarios, diagrammes d'enchaînement.
- Organique par des description de l'architecture physique
- Stratégique – pilotage : à partir de modèle d'élaboration de valeurs de régulation, des normes, des mesures
- Stratégique – fonctionnement : à partir d'automatismes, de modèles de régulation
- Stratégie – évolution : à partir de modèles d'élaboration de la décision.

La méthode est ainsi définit par une grille d'analyse systémique résumant neuf points de vue :

	Niveau activité	**Niveau fonctionnement**	**Niveau évolution**	
Point de vue fonctionnel	Fonctions ou missions correspondant aux activités opérantes	Processus enchaînant les activités pour réaliser les fonctions opérationnelles	Scénarios enchaînant des modes de fonctionnement	**Le système est**
Point de vue organique	Réseau opérant des organes réalisant les fonctions	Réseau logistique de mise en œuvre des activités	Réseau auxiliaire de changement de configuration	**Le système fait**
Point de vue stratégique	Pilotage : décisions d'équilibrage des fonctions (régulation)	Gestion : décisions d'adaptation des activités (transition entre états de fonctionnement)	Anticipation : décisions d'ordre stratégique (changement de mode de fonctionnement)	**Le système décide**
	Performance	**Stabilité**	**Intégrité**	

Figure 22 : Grille d'analyse systémique selon les neuf points de vue d'analyse d'un système.

Le modèle ainsi réalisé est complexe mais permet de simuler les différents comportements du système et par là même de modéliser l'expertise nécessaire.

L'APPROCHE COGNITIVE

Les principes de l'approche cognitive

La prise en compte du comportement humain dans la logique du comportement système a toujours été considéré comme un facteur d'accroissement du risque qu'on tente de réduire soit par la couverture de son intervention avec des technologies dites de sécurité, soit par la réduction de son intervention à des actions simples. Même si dans certains systèmes l'automatisation des contrôles et des actions peut être poussée jusqu'au remplacement de l'opérateur pour certaines fonctions de décision, plus le système tend vers la complexité, plus la combinaison de situation et de comportements possibles tend vers l'infini. Afin de pouvoir réagir face à des situations particulières il est alors nécessaire d'intégrer dans le système des composants ayant une capacité interprétative et créative. Or, le composant le plus utilisé reste à ce jour l'humain. Nous avons ainsi une situation qui peut paraître paradoxale ou l'opérateur humain est à la fois facteur d'accroissement et facteur de réduction du risque. Dans ce cas, il est nécessaire de rendre les comportements humain le plus prédictibles possibles, voire mesurables.

L'approche cognitive vise à travers une conceptualisation et une structuration des connaissances et des mécanismes comportementaux à prédire la réponse d'un système face à une situation donnée. Pour cela, la démarche consiste dans le principe à observer et à analyser des données afin de construire une connaissance et d'anticiper un comportement possible.

Mais, à la différence de l'ingénierie du risque qui à travers une décomposition du système et un cadre typologique va chercher à identifier les structurations de dangers, la démarche cognitive va faire de la situation l'objet de la connaissance pour conceptualiser et décrire une situation et construire une représentation qui permette de comprendre comment s'est organisée l'action qui a conduit à la situation observée.

L'approche cognitive n'est qu'une formalisation des raisonnements et de l'apprentissage que le cerveau pratique couramment. En fait, nous pratiquons une démarche cognitive sans le formaliser. Par exemple, la formation à la conduite d'un tramway, surtout au début de l'exploitation vise essentiellement à familiariser les nouveaux conducteurs avec quelques vérités :

- Il est impossible de changer de trajectoire pour éviter un obstacle, comme avec un bus,
- La réactivité du freinage d'une roue fer sur un rail est très différente. On apprend à un conducteur de tramway, ce qui est presque évident en ferroviaire : la vitesse du train se détermine essentiellement en fonction de sa distance d'arrêt.
- Enfin, le public immédiatement au contact du réseau continu à percevoir le tramway comme un bus et son silence ne correspond pas à la proximité du danger.

Au-delà des consignes de prudence, une des premières choses qu'on apprend à un nouveau conducteur est de chercher le regard des piétons pour s'assurer qu'ils ont perçus la présence du véhicule; pour cela, il faut faire usage du gong jusqu'à attirer l'attention de la personne avant de pouvoir continuer voire accélérer à nouveau. Il est donc courant de rouler avec des piétons en limite de gabarit, ceux-ci cherchant eux-mêmes le regard du conducteur.

En formation un formateur et son élève aperçoivent une jeune femme en limite du gabarit de circulation mais regardant dans la direction opposée. Le conducteur ralentissement et utilise son avertisseur sonore. lL jeune femme commence à tourner la tête puis les épaules et apparait un

très jeune enfant accroché à sa main, masqué jusque là. Le regard de la personne intercepté rien n'obligeait à freiner, et pourtant, la décision fût l'arrêt complet immédiat; cette décision était confirmée en parallèle par le formateur qui était déjà en position pour activer le frein de secours, pourquoi ?

Comme toute personne normale, la jeune femme a pivoté pour faire face au véhicule; cependant en tournant sur elle-même, l'enfant accroché à sa main allait lui effectuer un arc de cercle et engager le gabarit de circulation. Tous les conducteurs on remarqué inconsciemment qu'au coup de gong les gens pivotent sur eux-mêmes. Ce fait, même non formulé explicitement, était intégré par tous les conducteurs; aussi, lorsque l'enfant fût aperçu, naturellement le cerveau humain a anticipé son déplacement par rapport au pivot du corps de la mère et l'a placé devant la rame. Une rapide analyse faite immédiatement après l'incident a confirmé que le conducteur comme le formateur avaient suivi le même raisonnement. Ce raisonnement, est l'exemple parfait d'une approche cognitive :

- Observer la situation : la jeune femme, l'enfant en limite de trajectoire.
- Comprendre la situation : le mouvement de l'enfant provoqué par la rotation de sa mère.
- La situation cognitive : ici, la position de l'enfant après la rotation de la jeune femme.
- Qualifier la situation : la percussion de l'enfant par le tramway.
- Recadrer la situation : l'arrêt immédiat, avant même la fin du mouvement des piétons.

Il faut noter, que la jeune femme n'avait pas perçu le danger pour son enfant. Celui-ci faisait partie de sa "bulle" de protection, et même si elle avait eu conscience que cette bulle était en interférence avec la zone de circulation du tramway, elle n'avait absolument pas eu conscience du changement de position de son enfant pendant la rotation.

L'approche cognitive s'intéresse à des situations dynamiques, c'est-à-dire des situations où le comportement du système n'est pas simplement lié à sa structure et à sa matière mais aux situations passées et présentes.

A partir du moment où l'appréhension d'une situation est le résultat d'un processus de conceptualisation du réel, sa prise de conscience est dépendante du protocole d'observation. Les décisions d'interventions dépendent alors du sens et de la valeur que l'observateur accorde aux données perçues. Dans une démarche cognitive, la situation ne sera pas analysée en recherchant les causes qui ont permis d'y aboutir, mais en considérant une représentation de cette situation convenant à une action donnée. En d'autres termes, on ne cherche pas à déterminer ce qui va conduire exactement à une action mais à construire une représentation d'un contexte favorable et adapté à cette action.

MKSM: en exemple de méthodologie liée à la connaissance

MKSM (Method for Knowledge System Management) est une méthode d'analyse descendante développée par le CEA. Son objectif est de rendre les systèmes de connaissances intelligibles aux acteurs afin qu'ils les mettent en place eux même. A partir d'un ensemble de méthodes et d'outils de modélisation nécessitant peu de connaissances préalables, les phases de la méthode procèdent par raffinements successifs de l'analyse des connaissances, jusqu'à un niveau de division suffisant pour avoir une visibilité correcte sur les informations et les critères de décision pertinents.

MKSM est intéressante car elle cumule à la fois les caractéristiques d'une approche systémique et d'une perception des systèmes à travers les signes qu'ils envoient aux observateurs :

- le point de vue des signes, ou hypothèse sémiotique: les éléments caractérisant un système sont désignés sous le terme général de signes. Le système de connaissances associé est alors perçu comme un système de signes. Tout phénomène est perceptible selon trois niveaux indissociables : le référent ou signe (la manifestation), le signifié (la désignation), le signifiant (le sens) ou encore se perçoit selon trois dimensions : syntaxique, sémantique, pragmatique.
- Le point de vue systémique, pour lequel le capital de connaissances d'une organisation est un système au sens de la théorie du système général de J.L. Le Moigne [LE MOIGNE 77]. Un système s'observe selon trois points de vue indissociables : le premier, dit ontologique, considère le système comme "quelque chose" ; le deuxième fonctionnel, considère le système comme "faisant quelque chose" ; le troisième, dit génétique, considère le système dans son évolution, c'est le point de vue du devenir du système. MKSM choisit par convention la terminologie : structure, fonction et évolution.

La perception, l'étude, la modélisation d'un système se fait à travers une vision pondérée entre ces trois points de vue.

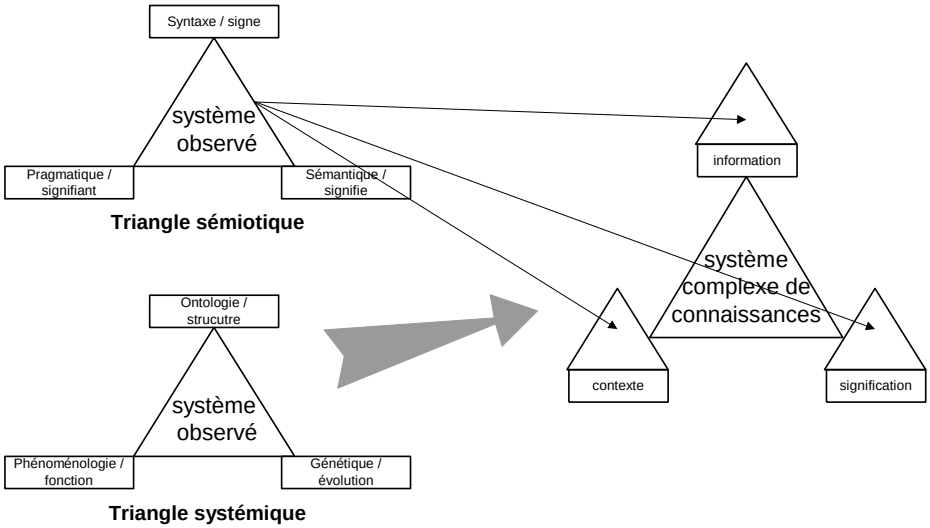


Figure 23 : Système de connaissance suivant les hypothèses sémiotique et systémique

SCIENCES DU DANGER ET CINDYNIQUES

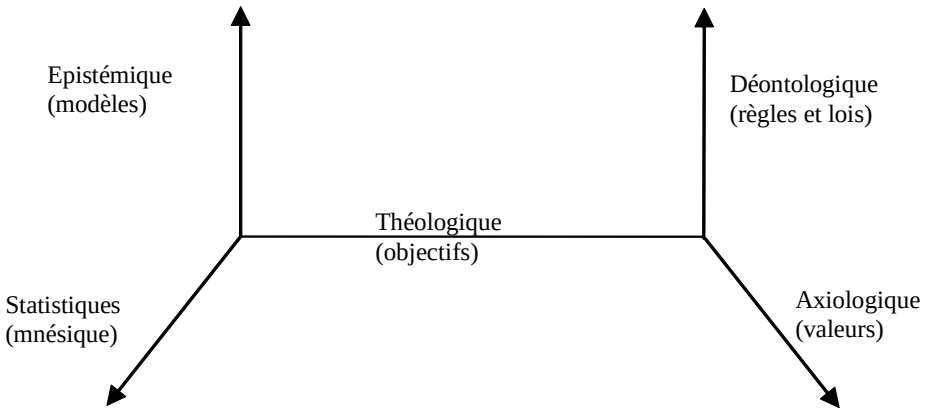
La science du danger se définit comme le corps de connaissances qui a pour objet d'appréhender les événements non souhaités. La constitution d'un tel corps a trouvé sa justification dans le fait que l'appréhension est centrée sur l'homme, la population, la nature ou le patrimoine, les centre d'intérêts se déplaçant, les techniques d'études et de prévention deviennent nécessairement différentes, et, si ces activités coexistent, elles s'ignorent ou se cloisonnent. La science du danger se définit plutôt comme un courant de pensée fédérateur, mais pas forcément

unificateur, des différentes connaissances. La réflexion menée poursuit un triple objectif pédagogique, opérationnel et culturel. L'objectif pédagogique passe par des stratégies de formation intégrant l'aspect transdisciplinaire. L'objectif opérationnel s'appuie sur la mise en œuvre d'une méthode appropriée d'analyse des risques (méthode MOSAR abordée ultérieurement). L'objectif culturel par une généralisation de la perception par l'extension des critères scientifiques, techniques et économiques de qualification du risque aux critères institutionnels, écologiques et culturels; c'est-à-dire une extension à des notions de sens, valeurs ou même d'éthique.

Les cindyniques représentent une approche purement systémique. Le développement de l'approche cindynique s'établit suivant deux axes :

- les cindyniques considèrent la forme la plus globale possible d'un système, rendant compte d'une activité humaine, de la façon dont elle est organisée, conduite et contrôlée.
- Les facteurs récurrents déclenchant ou aggravant des catastrophes, et, expliquant les erreurs commises par le système dans son ensemble.

Dans l'approche cindynique proposée par G.Y. Kervern [KERVERN 1995][KERVERN 1999], le système n'est plus analysé sous ses seuls aspects constructifs ou procéduraux mais en considérant le système comme un réseau d'acteurs évoluant sur un hyper espace danger produit de 5 espaces (données, modèles, objectifs, règles, valeurs). L'analyse cindynique est conduite sur une architecture à 7 niveaux : la base axiomatique, la structure de représentation (hyperespace cindynique), les situations comportant les opérateurs de transformation, le potentiel cindynique, l'évènement, le domaine de validité, l'intensité cindynique.



1ère dimension : faits de mémoire de l'histoire et statistiques.

2nde dimension : représentation et modèles élaborés à partir des faits

3ème dimension : les objectifs

4ème dimension : les lois, les règles, les normes, les standards et les codes (us et coutumes ?).

5ème dimension : les valeurs

Figure 24 : Hyperespace du danger

Le potentiel cindynique du système représente la propension d'un système à engendrer des dysfonctionnements, incidents, accidents, ou catastrophes, c'est-à-dire des Evénements Non Souhaités.

Les cindyniques ont identifié que les ENS, ont pour origine :

- un ensemble de facteurs réduit, généralisés sous la forme de Déficits Systémiques Cindynogènes (DSC) vus comme des trous dans le dispositif de connaissance et de pilotage des risques associés à un système,
- des Dissonances entre réseaux d'acteurs d'un même système ou de systèmes différents.

Les Déficits Systémiques Cindynogènes sont classées en trois grandes catégories :

- Déficits culturels : infaillibilité, simplisme, non communication, nombrilisme,
- Déficits organisationnels : subordination des fonctions de gestion des risques aux fonctions de production, dilution des responsabilités,
- Déficits managériaux : manque de retour d'expérience, de procédures écrites, de formation et de préparation aux situations de crises.

L'idée d'intensité cindynique croissante (du simple dysfonctionnement à l'apocalypse) permet de classer les ENS par impact croissant sur les cinq espaces. Entre deux systèmes, chacun muni de son hyperespace, on peut constater également des dissonances qui accroissent la propension de ce couple de deux systèmes

Importance de l'accident sur l'hyperespace cindynique à 5 dimensions

Incident : ne touche que les données

Accident : remet en cause les modèles

Accident grave : remet en cause les objectifs

Catastrophe : remet en cause les règles

Catastrophe majeure : remet en cause les valeurs

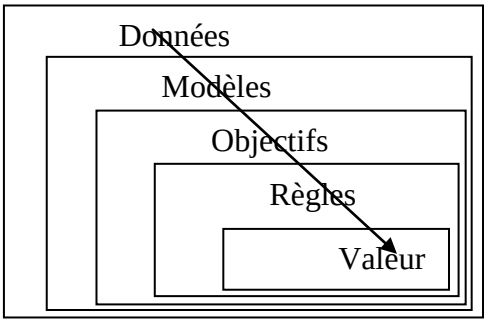


Figure 25 : Classification des conséquences en cindyniques

La base axiomatique permet de définir les propriétés des signes annonciateurs des accidents

- Axiome de relativité : la perception du danger est relative à la situation et à l'acteur qui la perçoit,
- Axiome de conventionalité : le risque est le produit occurrence gravité, sa mesure est subordonnée à des conventions entre les acteurs,
- Axiome de théologie : prend en compte l'explicitation des finalités des acteurs ce qui implique de préciser et hiérarchiser les finalités des acteurs,
- Axiome d'ambiguïté : les perceptions et estimations sont sujettes à des ambiguïtés. Ce dernier axiome est fondateur de l'hyperespace du danger. Le travail de prévention consiste à réduire les ambiguïtés,
- Axiome de transformation : les accidents et catastrophes sont révélateurs des ambiguïtés, ils opèrent une transformation brutale du contenu des 5 dimensions,

- Axiome de crise : la crise est une désorganisation des acteurs et des réseaux familier elle constitue une déchirure du système et implique l'organisation d'urgence d'un nouveau système d'acteurs qui vient compenser le premier,
- Axiome de nocivité : pose la nocivité inhérente à toute thérapeutique. Toute action sur la situation a des effets réducteurs mais aussi créateurs de dangers.

Pour compléter cette approche succincte il est intéressant de citer les cinq lois du danger définies par Kervern. L'intérêt de ces lois est qu'elles formalisent quelques principes qui resteront sous jacents dans la modélisation et dans l'étude des systèmes modélisés.

Loi de la réticularité cindynique : Le danger qui menace un individu est une fonction définie sur l'ensemble du réseau qui l'entoure. C'est-à-dire qu'il n'est pas possible d'apprécier le danger isolément mais qu'il faut tenir compte de l'ensemble de son environnement.

Loi de l'anti-danger : La gravité d'un danger est accrue par la sous-estimation de sa probabilité. L'accident est d'autant plus catastrophique que les victimes sont inconscientes du danger.

Loi d'invalidité cindynogène : L'excursion d'un système hors de son domaine de validité est cindynogène. Nous retrouvons là un des grands principes de la sécurité ferroviaire qui veut qu'un système ne puisse être de sécurité que sur son domaine de fonctionnement.

Loi de l'éthique cindynique : La qualité des relations dans un réseau est un facteur de réduction de danger. En d'autre termes, les tâches et les responsabilités sont elles clairement définies et comprises par l'ensemble du réseau.

Loi d'accoutumance au danger : avec le temps, la conscience d'un danger de faible probabilité diminue.

CONCLUSION

Nous avons vu au cours de ce chapitre que l'ingénierie du risque est un ensemble de techniques et de méthodologies dont l'objectif répond à trois objectifs complémentaires :

- Définir les critères identifiant le danger ou l'indésirabilité d'un événement ou d'une situation (détermination du domaine d'évolution).
- Définir le niveau d'acceptabilité du risque, c'est à dire déterminer les seuils à partir desquels un événement ou une situation est considéré dangereux (détermination des objectifs).
- Définir les moyens appropriés pour respecter les niveaux déterminés.

Ainsi même si l'ingénierie du risque s'appuie sur des outils mathématiques et scientifiques, la démarche reste une démarche managériale : détermination d'objectifs sur un domaine d'évolution donné et mise en œuvre des moyens appropriés.

La Maîtrise des Risques est à la fois une activité de projet et une activité décisionnelle. Les résultats de la première définissent le cadre décisionnel de la seconde. En effet, la première étape de la gestion des risques est de se donner une base qualificative permettant de déterminer en quoi un événement, une action, une situation représente un risque à couvrir ou non. L'exercice est difficile car nécessitant la prise en considération de critères humains, économiques et culturels qui sont souvent le résultat de l'histoire, de l'expérience ou d'une démarche législative. La seconde étape, souvent prépondérante dans la littérature car elle présente une plus grande richesse de moyens formels, est celle de l'identification et de la qualification. Cependant, si les outils, méthodes et approches globales restent communs, la qualification du risque et les mesures prises pour le réduire sont très dépendants du milieu social, technique, économique pour ne pas dire culturel sur lequel elles s'appliquent. De même, les actions, la stratégie appliquée ou les techniques employées suivent cette "préférence culturelle" comme la sécurité intrinsèque, très utilisée en ferroviaire et la défense en profondeur dans le nucléaire.

Quel que soit le domaine, industriel ou technologique, les études de sécurité ont toutes pour objectif unique d'identifier l'ensemble des chemins pouvant conduire à des situations réputées dangereuses. Nous observons que la recherche des dangers vise toujours à identifier des combinaisons mettant en œuvre : des objets, leurs relations structurelles, des flux. Cette recherche est conduite suivant trois grandes classes de méthodes : à base d'expertise, à partir des conséquences, à épuisement (identification systématique de toutes les combinaisons de comportement en réponse aux événements connus). La démarche appliquée est soit inductive, c'est-à-dire que sont recherchés les réseaux d'évènements (les coupes) conduisant à des situations dangereuses, soit déductive, c'est-à-dire que la réponse du système à des évènements déterminés est observée.

Qu'il soit inductif ou déductif, le processus réalise une analyse combinatoire visant à identifier des réseaux d'évènements. Une fois identifiés ceux-ci sont pondérés suivant leur probabilité d'occurrence et la gravité estimée des conséquences de la situation dangereuse résultante. Le couple gravité - occurrence devient alors le critère quantificateur du risque.

La démarche d'acceptabilité du risque, ou la classification de dangerosité, revient à décider quelles sont les valeurs du couple gravité occurrence admissible ou inadmissibles. Pour les situations inadmissibles, la démarche de réduction intervient alors :

- soit sur le réseau d'évènement lui-même pour l'interrompre ou le dévier,
- soit sur la probabilité d'occurrence d'un évènement du réseau, par prévention, de façon à rendre le risque final admissible,

- soit sur le critère de gravité par protection, c'est-à-dire en interposant une barrière, ou par éloignement des victimes potentielles.

Un autre radical commun de ces processus, est que les analyses sont conduites sur un système dont les limites sont connues et définies : composants, architecture, contexte, intervenants…

Seule des différences méthodologiques apparaissent dans la mise en œuvre des analyses, dans la façon d'appréhender le cycle de vie, le contexte ou les intervenants sur le système.

Une des limites essentielles de ce type de processus est que pour être efficace et admissible il est nécessaire que l'analyse soit la plus exhaustive possible. Qu'elle soit empirique ou systématique, l'analyse tente d'épuiser l'ensemble des cas, coupes ou évènements, de façon à garantir la maîtrise de la situation (et non de l'évènement). Au-delà d'une certaine complexité du système, seules les machines peuvent identifier la totalité des réseaux d'évènements. Cependant pour fonctionner les logiciels ont besoin que la description du système soit conceptualisée, formalisée et codée pour être exploitable. L'analyse se heurte alors à deux facteurs non négligeables, la distorsion apportée dans la description du système, et le coût de l'opération.

De même que pour les analyses de sécurité, les méthodes et techniques de couverture de risques sont essentiellement tournées vers la couverture de la défaillance technique ou de l'erreur humaine. Ce principe abouti en général à une recherche d'automatisation maximale du système à conduire ce qui reste acceptable à condition que l'environnement fonctionnel de celui-ci, que la technologie employée et que les objectifs primaires du système n'évoluent pas.

Les limitations de ces approches générales sont dues au fait que les méthodes d'analyses sont essentiellement analytiques et, en particulier, s'appuient sur une modélisation dont les concepts de base sont l'organe, la structure et surtout l'explication causale.

Aujourd'hui, les évolutions technologiques mais surtout la nécessité d'adaptabilité commerciale impliquent une remise en question du cadre fonctionnel dans lequel évolue le système et par conséquent du système lui-même. Pour reprendre le parallèle avec le domaine militaire, les systèmes de combat sont conçus pour répondre à une nouvelle menace. Cependant, le profil de mission évoluant une grande liberté d'action est laissée aux opérateurs et surtout à leur encadrement. L'entraînement permanent pourrait remplacer alors les évolutions techniques. Cependant le type de menace évoluant rapidement, il devient alors nécessaire de faire évoluer les performances des systèmes et par conséquent en parallèle le comportement des opérationnels. Dans le monde civil, nous sommes confronté à la même problématique. Il n'est plus possible de conserver la distinction entre la conception et l'exploitation d'un système, la maîtrise des risques devient alors une activité continue depuis les spécifications jusqu'à l'arrêt du système.

L'objectif principal de la maîtrise des risques systèmes n'est pas d'annihiler le risque mais de la maîtriser; c'est-à-dire de se prémunir par l'application de mesures ou de méthodes, contre l'occurrence de certaines situations, dites redoutées dont les conséquences sont jugées inacceptables. Néanmoins il est facile d'établir le constat suivant :

- plus le risque est maîtrisé, plus la probabilité d'occurrence d'accident diminue mais plus le prix de la protection (complexité, moyens,…) augmente.
- Si la probabilité d'occurrence d'accident diminue, à performances fonctionnelles égales, la gravité des conséquences n'en est pas affectée. Ce qui implique de dégrader les critères de performances influents sur la gravité si on désire réduire celle-ci.
- Enfin, et c'est surtout là le point qui est intéressant, un système est souvent conçu pour fonctionner dans un contexte bien déterminé dont on maîtrise les paramètres techniques (usure, environnement,…) mais plus difficilement l'évolution des paramètres humains.

Compte tenu, des limitations constatées, la maîtrise des risques, qui relève essentiellement de l'ingénierie se doit de dépasser ses limites conceptuelles pour évoluer vers des approches différentes dans l'appréhension de la chose observée. Pour dépasser ces limites il est nécessaire de se doter d'une représentation globale devant refléter le comportement, l'organisation et les relations qui régissent le système observé, mais aussi d'une représentation de la situation pertinente, permettant d'isoler les informations représentatives du risque. Cet élargissement implique d'intégrer sur un même plan les différents acteurs d'influence du système et d'ajouter aux éléments purement techniques sur lesquels on se concentre habituellement, les éléments humains et les éléments régulateurs. Cette transition peut se résumer ainsi :

- L'approche système, ou approche technique, qui à partir des besoins exprimés et d'un ensemble de connaissances construit une architecture technique assurant à des fonctionnalités déterminée et répondant à des prescriptions d'exploitation.
- L'approche systémique qui à travers une conceptualisation du système (des systèmes en général) établit des paradigmes comme autant de lois communes de comportement.
- L'approche cognitive, à travers une conceptualisation et une structuration des connaissances et des mécanismes comportementaux, cherche à prédire les comportements du système face à une situation donnée.
- Enfin, l'approche cindynique de plus haut niveau essentiellement liée à l'activité humaine, qui à partir de facteurs récurrents dans les origines des accidents propose non plus de se focaliser sur l'événement mais étudie les facteurs de déséquilibre à l'origine de l'apparition de ces événements.

Un des grands objectifs des approches dites systèmes est de couvrir les aspects transverses du système, c'est-à-dire de s'assurer que les relations entre les différentes entités ou les différents intervenants ne génère pas de risque supplémentaire ou ne remette pas en cause les mesures prises. Il existe différentes méthodes pour identifier et traiter ces aspects systèmes. La première consiste pour chaque composant à considérer ses interfaces connues en important ou exportant certains risques. En dehors de la tentation que chaque sous-système peut avoir d'exporter ses risques plutôt que de les couvrir, cette méthode reste très fortement influencée par le point de vue que chacun porte sur les autres. Les méthodologies prennent donc en considération ce phénomène par une couverture dite de niveau système de la gestion de la sécurité. Néanmoins, ce principe hiérarchise et structure les relations vis-à-vis de la sécurité, en fonction de la structure même du système; ce qui offre une vision incomplète des conditions menant à des situations dangereuses.

A la différence des méthodologies systèmes qui sont axées autour d'une définition structurelle (soit par les fonctionnalités, soit par l'organisation) et sur la recherche de défaillances, la vocation première de l'approche systémique est de sortir du cadre de l'objet opérant pour appréhender le système à travers son organisation globale. Or, appréhender quelque chose dans son organisation implique d'en connaître ses objectifs. Le système n'est plus vu comme une structure mais comme une entité agissante. Le concept de base de la modélisation systémique n'est pas l'objet, ou la combinaison d'objets stables (structure), mais l'action. La systémique offre là un terrain parfaitement cohérent avec la notion de risque, risque qui n'est lui-même que l'appréhension a priori d'une action et de ses conséquences. Ce point de vue sur le système par l'action offre une vision beaucoup plus étendue du risque car elle n'est pas limitée à la simple conséquence d'un événement mais intègre la capacité intrinsèque d'un système à produire une action. Par exemple, l'approche retenue pour le modèle MADS donne une bonne vision de cette nature de danger dans une modélisation systémique. Les approches systémiques et cognitives ont débouché sur des modèles et des méthodes dont l'intérêt est qu'elles visent toutes à intégrer les différents points de vue des acteurs, les différentes formes d'analyse des systèmes et les différents modèles de

représentation. Cette intégration n'est pas effectuée au détriment des spécificités mais cherche au contraire à établir des relations les plus universelles possible.

L'intérêt de l'approche systémique n'est plus à démontrer. Cependant, si les grands concepts et les paradigmes développés par celle-ci restent universels, le passage à un modèle de calcul repose encore aujourd'hui sur une description structurelle (fonctionnelle ou organique) qui reprend alors le point de vue du modélisateur. Ce phénomène est du au fait que les méthodes développées viennent essentiellement en complément des approches analytiques et non en remplacement.

Le principal apport des démarches systémiques est de mettre l'acteur humain et l'organisation au sein de laquelle il évolue au centre des problèmes de la gestion des risques. La prise en compte simultanée d'éléments techniques, environnementaux, humains et régulateurs crée une problématique ardue que l'on résume souvent sous l'appellation de système complexe. La notion de complexité ne répond alors pas à une définition précise mais reflète le sentiment qui se dégage face à un système avec des interrelations nombreuses, des phénomènes aléatoires, des imbrications de niveaux, une hétérogénéité des objets représentés et des connaissances mises en œuvre. Les méthodes qui appliquent des approches systémiques proposent une organisation des données selon un cadre formel mais non une modélisation des concepts.

Enfin, la démarcation que proposent les cindyniques est importante. Au-delà, de la définition d'un hyperespace du danger ou de l'identification des conditions d'apparition des dangers, la cindynique est la discipline qui a entièrement franchi le pas de l'approche systémique et qui considère un système essentiellement par ses projets et non plus seulement par ses objets ou ses fonctions.

VERS UNE NOUVELLE APPROCHE DE MODELISATION

INTRODUCTION

La lecture de la première partie de ce mémoire a montré que l'essentiel des techniques et outils de la maîtrise des risques sont essentiellement fondés sur des approches analytiques car celles-ci ont d'abord comme objectif la connaissance de l'objet opérant.

Si les approches descriptives, comme SAGACE, organisent la démarche et l'analyse, les approches analytiques définissent les éléments opérants, les flux et l'environnement de façon à analyser un comportement. Ces approches analytiques utilisent la connaissance générale ou le retour d'expérience pour identifier des situations dangereuses et les événements pouvant y conduire, et des outils formels pour les processus de gestion du risque. Ce qui constitue le domaine de l'ingénierie du risque. Il est possible d'affirmer que le domaine de l'ingénierie du risque compte aujourd'hui tous les outils d'analyse et de calcul nécessaires à la qualification de situations par le critère gravité-occurrence. Les normes et textes réglementaires définissent l'objectif socio économique et les outils permettent l'analyse de situations et le calcul d'occurrences. Les méthodologies et règles de l'art orchestrent les activités de gestion proprement dites : affectation, spécification, conception, traçabilité, contrôle… Néanmoins, en dépit de toutes les méthodologies développées, l'ingénierie du risque est essentiellement tournée vers l'équipement et ses modes opératoires et demeure ainsi confrontée à un certains nombres de limites que les outils et méthodologies ne permettent pas de dépasser :

- la spécificité des modèles produits,
- l'évolutivité des modèles,
- la prise en compte de l'humain en tant que composante système,
- l'évolution des connaissances.

La spécificité des modèles produits résume en fait la problématique qu'induit la spécialisation des analystes ou des concepteurs sur un domaine technologique et sur son environnement. En effet, les démarches analytiques tendent à répondre au besoin de compréhension d'un système ou d'un phénomène par la production d'un objet symbolique représentatif du système observé, établi à partir d'une décomposition de celui-ci. Le modèle, s'il est pertinent, doit permettre de comprendre par la simulation et l'analyse de sa structure, le phénomène ou le système observé. Si cette vision technologique est parfaitement suffisante lorsqu'il s'agit de qualifier un système essentiellement matériel, elle devient très réductrice lorsqu'il s'agit d'évaluer un système complexe ou à forte composante humaine. C'est à cette problématique qu'ont cherché à couvrir d'abord les approches système puis les sciences du danger, les sciences cognitives et les cindyniques.

Au vu de ce qui a été développé précédemment, il est légitime de démontrer ce que l'on peut encore apporter. Posons nous la question de ce que nous attendons d'un modèle aujourd'hui, et comment il s'inscrit dans la démarche de management du risque.

LES OBJECTIFS D'UNE NOUVELLE APPROCHE

A ce jour, un modèle offre à travers sa représentation de l'existant (ou de l'existant projeté) une capacité prédictive par une vision du futur ou du possible. Le paramétrage et la possibilité d'identifier certains radicaux (indicateurs) fournissent de la souplesse au modèle et permettent une certaine adaptabilité à des contextes différents. Dans le cadre d'une analyse des causes des dangers, des modes de défaillances, ou même, des conditions aux limites, le modèle remplit parfaitement ses objectifs. Or nous avons vu dans la présentation des approches systèmes, puis des

approches systémiques, que la simple analyse d'un système figé était insuffisante et devait être complétée par une politique de gestion de la sécurité. Le management de la sécurité est une activité complète comprenant une analyse *stratégique* (connaissance de l'état de l'art, vision des futurs probables et possibles), une analyse *tactique* (vision des solutions et moyens), et une *tenue de situation* (contexte au sens le plus large). On constate alors que si cette activité veut pouvoir s'appuyer sur un modèle celui-ci ne peut plus se poser comme une simple représentation d'un système à un instant donné, mais doit être capable de représenter le système tout au long de son cycle de vie; ainsi le modèle passe du statut d'outil d'analyse à celui de moyen d'aide à la décision. Le modèle produit se doit alors de permettre une représentation simplifiée et unificatrice d'un problème ; en effet, toute l'énergie de l'analyse doit rester concentrée sur l'activité de management : réflexion et décision. Il devient nécessaire de repousser les limites en élargissant les objectifs visés.

Nous avons vu à travers la première partie de ce mémoire que les approches complémentaires proposées cherchent chacune à combler une ou plusieurs lacunes de l'ingénierie du risque :

- la différenciation des intervenants techniques, ou des domaines technico-culturels,
- la prise en compte du comportement humain ou de l'activité humaine,
- l'élargissement de la vision structurelle du système à son organisation.

Chaque approche tente de ne pas sacrifier l'acquis en le complétant ou en essayant de le fédérer.

A travers l'approche de modélisation proposée par la suite nous allons tenter d'intégrer ces diverses préoccupations dès la définition des modèles. En premier lieu, le système n'est plus considéré comme un ensemble structuré mais plutôt comme un potentiel d'action. Pour permettre la communication il est nécessaire de définir un modèle conceptuel unifié au sens du partage de la compréhension et de l'appréhension des concepts développés. Au même titre que les sciences du danger, une nouvelle modélisation doit servir de pivot à l'ensemble des intervenants en gestion de la sécurité en conception et en exploitation, en favorisant naturellement la communication et la communauté de point de vue. A ce titre, il est nécessaire que le système puisse être modélisé comme une organisation composée d'une activité humaine, d'une base de connaissance et d'éléments technologiques. Pour éviter que les résultats soient remis en cause à chaque étape de la modélisation les transformations entre le modèle conceptuel, le modèle de représentation et le modèle de calcul associé doivent être minimisées.

D'un point de vue plus pragmatique, un des premiers objectifs de ce travail de recherche est donc de proposer un modèle depuis la représentation conceptuelle jusqu'au modèle de calcul informatique reste le plus universel et le plus proche possible des concepts utilisés par les modélisateurs et d'utiliser cette représentation systémique dans les analyses de sécurité et les processus de gestion des risques.

LES CONTRAINTES DE LA MODELISATION

La conceptualisation

Le processus de modélisation est souvent confondu avec celui d'analyse qui consiste en la décomposition d'un phénomène en éléments plus faciles à appréhender. En réalité, la modélisation vise à décrire un problème puis sa solution à travers une abstraction qui en établit une représentation simplifiée. Cette opération permet à des observateurs de décrire un phénomène à partir de représentations conceptuelles, afin de le comprendre et de le simuler.

L'action de modéliser n'est pas neutre et la représentation du système observé ne peut alors pas être disjointe du travail du modélisateur. La définition d'une approche modélisatrice doit donc s'affranchir des "biais" de transformations inhérentes aux actions des modélisateurs :

- la distorsion créée par la perception et la restitution du phénomène perçu,
- la compréhension et le sens des concepts dégagés,
- la transformation d'un phénomène observé au cours d'une démarche récursive,
- la compréhension et le sens porté par la représentation symbolique du modèle produit.

Etant donné qu'un modèle n'est avant tout qu'une représentation intellectuelle puis ensuite symbolique d'un monde observé, il est nécessaire de scinder la démarche de modélisation en deux opérations complètement indépendantes : la conceptualisation et la représentation.

Dans une démarche de modélisation la conceptualisation permet de dégager une représentation du monde réel sous des formes logiques généralisées et utilisables: le méta-modèle. Le méta-modèle est une représentation formelle des concepts de base de la modélisation (syntaxe, sémantique…) et des règles qui régissent leur utilisation. Ainsi, si le contenu d'un modèle dépend du système ou du phénomène observé, la forme du modèle ne dépend que du méta modèle.

Le méta modèle est le résultat d'un premier travail d'observation. Ce travail porte sur l'identification et la définition des concepts fondamentaux qui forment les éléments de base de la modélisation d'un système. Ces concepts fondamentaux constituent des éléments génériques échangeables par les différents observateurs d'un système ou d'un phénomène; d'où l'importance des concepts choisis et de la représentation sémantique qui leur est associée. On attend de la construction d'un méta modèle un gain dans l'abstraction du système par la généricité des concepts de base comme facilitation dans l'identification éléments constitutifs du système observé et dans la simulation des comportements.

Si la conceptualisation s'attache essentiellement aux objets réels et à la forme sous laquelle ils peuvent être représentés, la démarche de représentation doit viser à décrire le système étudié à partir des concepts du méta-modèle pris comme autant de descriptions de référence. Ainsi si le contenu du modèle fournit une image d'un système observé sous un point de vue particulier, la forme de ce modèle ne reste qu'une représentation conceptuelle de celui-ci établie dans un cadre formel donné ou choisi.

La définition du méta modèle doit prendre en compte une double problématique : la compréhension du réel et la robustesse du modèle de représentation, ce qui se traduit par l'obligation de respecter les objectifs suivants :

- lisibilité des concepts,
- fiabilité du formalisme retenu,
- neutralité de la représentation,
- confiance dans les résultats produits.

Ce dernier point étant un corollaire des trois précédents.

La *lisibilité* des concepts est un critère capital dans la définition des concepts fondamentaux. En effet, chaque méta modèle définit des règles et des représentations des éléments de modélisation, par exemple la modélisation fonctionnelle utilise les concepts de fonction et de tâches, la modélisation objet les concepts d'entités et de relations, pour représenter un système. Si nous voulons modéliser la dynamique d'un système il est alors nécessaire d'établir une description permettant de représenter la dynamique du système à partir de concepts intellectuellement et mathématiquement (par conséquent informatiquement) manipulables. La lisibilité des concepts doit permettre un échange pluridisciplinaire autour des concepts définis, elle doit minimiser le biais induit par les transformations dues à la conceptualisation mais aussi à la déconceptualisation.

La lisibilité des concepts doit aussi permettre la production d'une application informatique sans induire de nouveau un biais dans cette transformation.

La *fiabilité* du formalisme : la conceptualisation va définir un cadre de travail sur lequel va être projeté le système observé et ensuite simulé sa dynamique; il est donc nécessaire que les mécanismes mis en œuvre soient démontrés.

La *neutralité* de la représentation: La méthodologie et le formalisme proposés ont pour objectif de pouvoir conduire des analyses pendant toute la démarche de modélisation puis d'exploitation du modèle. Si ces activités relèvent du domaine de l'expertise et de l'expérience, le cadre descriptif choisi doit rester aussi neutre que possible dans l'observation.

Résultat du respect des trois premières contraintes, la *confiance* dans les résultats produits signifie que le modèle ne doit pas avoir à être évalué mais que seuls les résultats doivent présenter un intérêt.

Complexité, raffinage et décidabilité

Cette problématique trouve ses origines dans le fait qu'un système complexe a un comportement résultant lui-même de la somme de comportements complexes qui impliquent que le modélisateur est confronté à une triple problématique :

a) *la complexité* proprement dite qui s'établit à partir des interrelations entre les composants appartenant au système. Cette complexité n'est pas due à la quantité de relations existant entre les composants mais au fait que celles-ci ne représentent pas forcément un lien fonctionnel direct entre eux et trouvent leur origine dans la structure même de l'environnement ou du système.

b) *la variété* qui caractérise le nombre de comportements possibles à partir des interrelations entre composants. La notion de variété d'un système est une donnée initiale, structurale et fonctionnelle, qui recouvre à la fois la différenciation des éléments et la différenciation des agencements et des relations entre ces éléments. A la différence des évolutions qui caractérisent les comportements irréversibles (qui transforment le tissu relationnel), la variété recouvre tous les états et les comportements possibles d'un système qui sont réversibles. La variété peut alors augmenter par l'apport de nouveau composants, mais aussi en poussant la spécialisation de composants déjà présents. Elle peut dépendre de l'inversion ou de la création de nouvelles relations, établissant des états différents. Enfin, à partir de certains seuils, l'augmentation ou la diminution des échanges entre les composants peut amener des organisations différentes. En conclusion, on peut dire que la variété est due autant au nombre et à la structure des composants que l'organisation des relations entre ceux-ci.

c) *la redondance* qui comprend la redondance structurale et la redondance fonctionnelle (polyvalence). La redondance structurale est le résultat de l'indifférenciation de certains éléments du système vis-à-vis d'une action. La redondance fonctionnelle est plus complexe et fait intervenir une certaine polyvalence des éléments du système, ainsi que les capacités de communication et de coordination inter-éléments présents dans le système. Cette notion de redondance, couvre à la fois la polyvalence des composants, mais aussi des potentialités polymorphes pouvant se révéler au cours des interactions avec l'environnement ou par apprentissage.

L'intérêt essentiel d'une modélisation est la réduction de la complexité par l'appréhension du global vers le particulier par raffinage. Cet aspect est capital dans l'étude et l'analyse d'un système. En maîtrise des risques, l'impossibilité d'anticiper toutes les situations dangereuses ou toutes les conditions qui peuvent y mener dès la conception conduit à décomposer les systèmes en sous système dont on maîtrise le cœur et les interfaces. Néanmoins, si une telle démarche de raffinage permet de réduire la complexité des éléments manipulés par des approches récursives de

généralisation et spécialisation elle introduit en retour un doute sur la suffisance de la profondeur de l'analyse et donc sur la décidabilité des résultats obtenus.

L'approche de réduction de la complexité doit donc être une approche qui permette de garantir le résultat à chaque niveau de l'abstraction en évitant au minimum de remettre en cause l'environnement de l'élément modélisé. Etant donné que la perception qu'on a d'un système n'est pas forcément la plus macroscopique, la modélisation doit alors permettre, une démarche de particularisation offrant une capacité d'appréhension du global vers le particulier et inversement, la possibilité de globaliser la perception d'un système depuis la connaissance d'un élément particulier.

L'imposition d'une approche de conceptualisation de caractère fractal est déjà une première réponse au problème de décidabilité. Ainsi, la démarche de particularisation fractale peut se faire sur chaque composant individuellement sans remettre en cause la globalité du modèle, et de même une démarche de généralisation fractale permet de conserver les résultats acquis pour le niveau supérieur. Cette démarche de décomposition - recomposition fractale ne peut se faire qu'à travers une structure générique répétée et répétable à l'infini, directement transposable en modèles, à travers de laquelle il est possible de représenter un système quelconque.

LA VISION D'UN SYSTEME

La démarche analytique : une vision limitée de la dynamique d'un système

Les définitions les plus simples qu'on puisse donner d'un système sont celle de L. de Bertallanfi, « ensemble d'éléments en relations les uns avec les autres », ou celle du *Webster'dictionnary*, du même ordre « ensemble organisé d'éléments soumis à des interactions mutuelles, cet ensemble faisant l'objet d'un contrôle ». L. de Bertallanfi a émis une *théorie générale des systèmes* fondée sur cette définition très générale réduisant la notion de système aux seules relations entre ses éléments.

La notion de système peut aussi se définir suivant différentes approches :

- Psychologie de la forme : le tout est perçu avant que les éléments ne soient distingués. Ceux-ci ne sont ensuite perçus qu'en fonction du tout,
- Mouvement structuraliste : les éléments sont définis par la structure à laquelle ils appartiennent.
- Mathématique : la dynamique des systèmes linéaires est issue de la constatation que de nombreux ensembles peuvent être caractérisés par des boîtes noires dont les interactions sont décrites par des fonctions de transfert largement indépendantes de la nature technologique des boîtes,.
- Formalisme indépendant du support matériel : modélisation par parallélisme entre le mode d'assemblage de dispositifs physiques et les fonctions qu'ils peuvent exécuter du fait de leurs interactions.
- Le système peut aussi être caractérisé par l'imbrication de disciplines multiples ou par ses objectifs.

L'ensemble de ces approches convergent vers une définition intégrant :

- Une conception circulaire de la causalité (boucles de rétroaction),
- Une décomposition en ensembles organisés dotés d'autonomie mais interdépendants,

- Une attention portée aux relations entre éléments plutôt qu'aux attributs de ces éléments.

L'ensemble se résume en disant qu'un système est une entité autonome par rapport à son environnement, organisée en structure stable (repérable dans la durée), constituée d'éléments interdépendants, dont les interactions contribuent à maintenir la structure du système et à la faire évoluer. Enfin, C. Lievens dans [LIEVENS 1976] a donné une définition approprié à l'analyse sécurité : un système est un ensemble organisé et articulé dont les éléments fonctionnent en synergie pour accomplir une ou plusieurs missions et dont le niveau de complexité technique est d'un ordre de grandeur nettement supérieur à celui de chacun des constituants. En fait, la notion de système vise à saisir globalement des problèmes complexes et les apports épistémologiques visent à en formaliser et à unifier l'approche descriptive de ces systèmes. Elle implique l'utilisation de modèles qui permettent de représenter la structure des éléments qui constituent les ensembles, ainsi que leurs interactions à partir de représentations mathématiques (analyse de système, dynamique de système) et des outils de simulation (modèles d'équations différentielles, systèmes multi-agents). Toutes les définitions données d'un système ont pour point commun de voir celui-ci comme un ensemble d'unités actives organisées et solidaires, en interaction entre elles et en interaction avec un ou des environnements par l'intermédiaire de flux identifiables qualitativement et quantitativement. Ces unités actives sont généralement appelées des processus, ou éventuellement s'ils sont vus en tant qu'objets ou organes, des processeurs. En modélisation, le processus ou le processeur est généralement représenté par une boite noire, l'objet processé ou matière est lui-même représenté par les transactions entre processus : les flux. L'objet est un intrant ou un extrant suivant qu'il est utilisé ou produit par le processus. Chaque action est caractérisée par le processus, ses intrants et ses extrants.

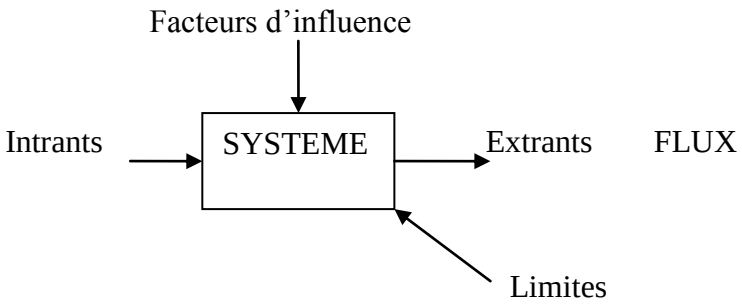


Figure 26 : Principe de l'analyse système

Un processus peut être une opération élémentaire mais aussi une combinaison plus sophistiquée d'opérations. Les limites d'un processus se définissent non pas par les opérations mais par les intrants et les extrants. Cette limite n'est pas figée. Il peut être intéressant à un moment donné d'avoir une vision globale d'un processus pour ensuite raffiner son comportement.

Le monde réel comprend différents types de processus comme la transformation, réaction, stockage, restitution, décision,…Tous ces processus respectent la forme présentée, la différenciation se fait par la nature des entrées et des sorties. La notion de causalité n'intervient jamais. La connaissance des processus s'établit alors à partir du processus lui-même, de la nature des sorties ou de la nature des entrées.

Dans une approche analytique la conception ou l'étude d'un système se fait à partir de deux structures statiques : la structure fonctionnelle et la structure organique. La structure fonctionnelle

établit une architecture de la dynamique des procédés mis en œuvre pour remplir un objectif donné, qui est soit celui du système - on parle alors de fonctions principales - soit essentiel à la bonne marche du système – on parle alors de fonctions de service. Cette description définit des opérations (entités fonctionnelles) et des flux (relations fonctionnelles). Nous avons là la première dimension de description statique d'un système : sa dimension fonctionnelle. La description organique établit une organisation mise en œuvre pour effectuer chaque opération de la description fonctionnelle. Cette description définit alors des entités organiques (ressources, liens, agents) et les relations organiques (architecture matérielle, organisation…). Nous avons là la seconde dimension de description statique d'un système : sa dimension organique.

Cette première organisation montrant de façon simplifiée qu'un processus se définit par des éléments organiques (opérations, paramètres, éléments physiques) et des éléments fonctionnels (flux, opérations, variables aléatoires) dont les interactions sont présentées le à deux entrées *fonctionnelle* et *organique* présenté ci-dessous :

		Dimension fonctionnelle		
		Entrées	**Opérations**	**Sorties**
Dimension organique	**Agents**	Règles Environnement Commande	Paramètres	Commandes Energie Informations Connaissances
	Flux	informations matière	Comportements opérations	
	Ressources	Connaissances énergie	Objets techniques Architecture	

Ce tableau n'étant que la description du modèle organo-fonctionnel suivant :

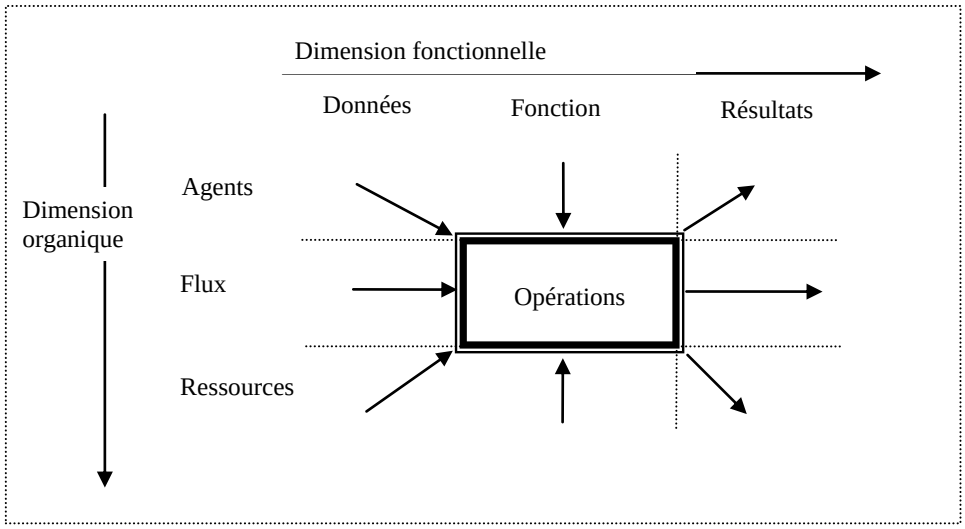


Figure 27 : Modèle organo-fonctionnel

La vision d'un système à un instant donné est celle d'un espace d'objets et de leurs propriétés respectives vue à travers sa description structurelle et sa description fonctionnelle. A partir des relations alors identifiées par les liens entre les processus on en déduirait une description comportementale. Cette généralisation fournit comme principe que :

- La dimension fonctionnelle est généralisée : fonctions données et résultats
- La dimension organique est localisée au processus : agents, flux, ressources.

Ces deux dimensions, largement utilisées dans une approche analytique, permettent de décrire un système et la cartographie de sa dynamique sous forme d'entités, les processus et de relations dans un espace statique mais n'offre pas la capacité d'élaboration d'actions inconnues a priori.

La démarche systémique : une vision d'un système par sa dynamique

L'approche systémique repose sur 3 axiomes, représentatif de l'appréhension d'un système par sa dynamique :

- *l'axiome téléologique* ou de *synchronicité* : un phénomène modélisable est perçu Action Intelligible ; c'est-à-dire non erratique, présentant une forme quelconque de régularité.
- *L'axiome d'irréversibilité téléologique* ou de *diachronicité* : un phénomène modélisable est perçu Transformation, formant projet au fil du temps.
- *L'axiome d'inséparabilité* ou de *récursivité* : un phénomène modélisable est perçu conjoignant inséparablement l'opération et son produit, celui-ci pouvant être producteur de lui-même.

Ces trois axiomes ont une signification et une importance extrêmement forte qui peut se résumer ainsi :

- un phénomène modélisable présente une forme d'organisation,
- cette organisation n'est que la déclinaison d'un projet d'action,
- l'action est le résultat d'un projet organisé et de l'environnement au moment de l'action,
- un système ne peut se définir par une image des objets à un instant donné.

De manière générale, l'approche systémique s'intéresse aux phénomènes, en posant que celui-ci est l'expression de la dynamique d'un système et se définit à partir d'un projet initial, ce projet initial étant lui-même un ensemble d'objets organisés projectivement à un projet d'action.

La modélisation systémique convient que tout système ou phénomène complexe peut être représenté par un système d'actions multiples. Le concept général représentant l'action est le processus. Le processus définit les changements qui affectent les objets, ces changements pouvant intervenir dans le temps, l'espace, la forme ou la nature. Le concept de processus évoque toujours une relation objet processé (qui subit les changements), objet processeur (qui produit les changements), et la description de ces changements. Chaque action sera alors caractérisée par le processus à un instant donné, ses intrants et ses extrants à cet instant. Les parties se définissent et existent ainsi par leurs relations mutuelles et non par ce qu'elles sont, le système n'est pas vu par ses objets mais par son organisation en vue d'une action.

Pourquoi cette vision d'un système par l'action est-elle fondamentalement différente de l'approche analytique ?

Principalement parce que le système n'est pas perçu par son organisation et sa structure (aspect organique) mais par ses actions (aspect fonctionnel). Dans ce cas, l'approche systémique postule qu'une action n'est pas le résultat d'une organisation mais que le système s'organise afin de produire ces actions. Dans une approche de maîtrise des risques cette démarche est très intéressante car le système n'est plus seulement vu à travers ses défaillances mais comme producteur potentiel d'actions dont certaines sont indésirables, et ce, quelles que soient la structure et l'organisation de celui-ci.

Si nous considérons un système purement technique, comme un automate, quel que soit le niveau de sophistication des actions réalisées celles-ci sont programmées et restent parfaitement

déterminées. La réponse d'un système technique aux sollicitations est connue. La modélisation consiste à représenter la combinaison ces (sollicitations – actions) sous une forme simplifiée, représentative et intelligible.

Considérons un système dont le comportement possède une certaine autonomie. Il élabore lui-même ses comportements en fonction de sollicitations internes ou externes, sans en être complètement dépendants. Il n'est plus possible d'appréhender ce système à travers une logique (sollicitation – action). Cette autonomie est la caractérisation du fait que le système a ses projets propres qui motivent ses comportements; il n'est pas "ballotté" par les événements mais adapte ses comportements à ses propres finalités. Le système est capable d'actions construites de façon pertinente vis-à-vis d'un projet d'action. D'après l'axiome de récursivité, on peut dire que le projet se transforme en fonction des actions réalisées. La conséquence en est que le système ne se définit pas uniquement à partir d'un processus basé sur un objectif, mais comme la combinaison d'un acquis (les comportements passés), d'un présent (les sollicitations de l'environnement) et d'un futur (les intentions d'actions avec leurs conséquences telles qu'elles sont anticipées par le système), ce qui est la vraie expression de la dynamique d'un système.

C. Lievens dans [LIEVENS 1976] avait déjà proposé une classification des systèmes en fonction de certaines de leurs capacités à se transformer. Une première classification des systèmes était effectuée en fonction de leur structure interne, en fonction du fait que le système soit naturel ou artificiel (mécanique), statique ou dynamique. Une seconde classification permettait de différencier les catégories par les relations du système avec l'environnement :

- Le système échange des informations ou de l'énergie avec l'extérieur,
- Le système présente une capacité d'adaptation aux perturbations extérieures sans laisser détruire sa structure (rétroaction de 1er ordre),
- Le système a une mémoire sélective lui conférant une capacité tactique : réaction réfléchie face à l'environnement en tenant compte de ses modifications (rétroaction du 2nd ordre),
- Le système a une capacité d'apprentissage lui conférant une capacité stratégique : adoption de nouveaux comportements pour atteindre son objectif (rétroaction du 3ème ordre),
- Le système a une volonté et une imagination créatrice lui permettant de modifier ses objectifs et son environnement externe,
- Le système a la capacité de changer ses propres structures.

Il faut noter que cette classification est effectuée sur la base d'une approche structurelle, et, présente le comportement sous un aspect contrôlé et causal.

Un autre principe important de la systémique est le principe d'entropie et en particulier d'irréversibilité : un système va toujours naturellement d'un état instable à un état stable et jamais l'inverse. Pour obtenir la situation inverse, il est nécessaire de faire un apport au système (énergie, information). La relation d'un système à son environnement est donc caractérisée par deux phénomènes :

- une transaction du système avec son environnement : le flux,
- un changement dans la stabilité du système mettant en évidence une capacité d'influence de l'environnement : le champ.

L'approche retenue pour le modèle MADS illustre ce principe d'une modélisation systémique dans l'analyse des sources de dangers. Tout processus émet des flux qui sont vus comme un chemin de transfert entre deux processus. Il relie donc deux sous-systèmes, appelés source et cible. La notion de champ définit "une capacité d'influence": c'est l'ensemble des éléments qui influent sur le processus sans en faire partie. Les flux sont essentiellement des flux de

matière, d'énergie ou d'information mais la typologie peut être étendue, par exemple, aux flux cognitifs.

Les processus de source ou de cible sont des processus de forme (transforme le flux) ou de nature (transmute le flux), les processus de champs sont des processus de temps ou d'espace.

Pour éclairer ce principe considérons l'exemple d'un véhicule automobile en déplacement sur une route. L'entité principale du système va donc être le processus de conduite qui établit et maîtrise les changements de position du véhicule sur la route. Un conducteur est un système stable. Le véhicule conduit par un conducteur sur une route est un autre système stable.

Le conducteur boit de l'alcool. L'alcool injecté dans le système conducteur par le processus *boire* va modifier l'état du conducteur. Le conducteur va avoir un autre comportement. L'apport d'alcool au conducteur a établi un flux de danger avec l'environnement qui a, sans jeu de mot, modifié la stabilité du système. Par contre, le changement de comportement du conducteur au volant va conduire à une remise en cause de la conduite du véhicule, le système de conduite va quitter son état stable; l'alcool est un champ de danger pour le système de conduite d'un véhicule.

Si d'un point de vue purement représentatif, nous retrouvons à travers les concepts d'objets et de processus présentés les radicaux communs aux approches systèmes et systémiques, étant donné le poids accordé à la structure du système en regard de son comportement, ces concepts restent insuffisants pour décrire la dynamique d'un phénomène. Etant donné qu'une action unitaire est le résultat d'un processus à un instant donné et de son environnement à cet instant (l'environnement est vu au sens le plus large englobant objets processés et objets processeurs en relation), l'exécution d'un projet ne peut se définir que comme une collection de processus, de leurs environnements respectifs à l'instant de chaque action du projet. La limitation des approches analytique provient du fait qu'elles cherchent à modéliser la dynamique d'un système à partir d'une vision statique de celui-ci et qu'elles offrent ainsi une vision réduite de sa dynamique. Or, par dynamique d'un système il ne faut pas simplement comprendre ses actions et réactions mais aussi ses évolutions; c'est-à-dire que la dynamique d'un système est un complexe : comportement – transformation.

CONCLUSION

La démarche systémique part du principe qu'il faut d'abord chercher à identifier les problèmes à résoudre avant de modéliser le phénomène. La démarche systémique va donc chercher à produire un modèle projectif de référence à partir duquel le modélisateur va établir un projet de représentation du phénomène observé. Le modèle est alors obligatoirement lié à l'association modèle projectif – modélisateur. C'est l'objectif de la méthode MADS qui propose un cadre permettant d'identifier les sources potentielles de problèmes (les champs de danger) afin de modéliser leur influence sur le comportement du système.

La démarche analytique tend à répondre au besoin de compréhension d'un système ou d'un phénomène par la production d'un objet symbolique représentatif du système observé établi à partir d'une décomposition de celui-ci. Le modèle établi, s'il est pertinent, doit permettre de comprendre par la simulation et l'analyse de sa structure, le phénomène ou le système observé. Néanmoins le point de départ de cette approche reste une observation statique du système : structures organiques ou fonctionnelles. Ainsi l'essentiel des techniques et outils de la maîtrise des risques sont basés sur des approches analytiques car celles-ci ont d'abord comme objectif la connaissant a priori de l'objet opérant du système. Les analyses de risques utilisent la connaissance générale ou le retour d'expérience pour imaginer les environnements de l'élément opérant et identifier des situations dangereuses et les événements pouvant y conduire.

On peut synthétiser les deux démarches ainsi : la démarche analytique cherche à modéliser le système pour à partir de la connaissance simuler son comportement, la démarche systémique modélise le comportement aboutissant à un problème connu. On a donc deux méthodes qui dans leur mise en œuvre actuelle semblent très proches et qui pourtant relèvent d'une démarche méthodologique et d'une démarche de conceptualisation opposées.

L'objectif de la recherche a donc été de proposer une méthodologie et ses outils sur la base d'une approche entièrement systémique, c'est-à-dire à partir du comportement, permettant de conceptualiser un système indifféremment à partir de ses caractéristiques intrinsèques qu'à partir du résultat de son comportement. Pourquoi systémique ? Car, cette approche pose que le système trouve sa stabilité dans sa finalité et que la poursuite du ou des projets est maintenue par des évolutions de son organisation. L'organisation et les relations que nouent les éléments actifs entre eux font émerger de nouvelles propriétés mais corollairement peuvent induire la perte de certaines potentialités intrinsèques de ces parties. Nous retrouvons là les préoccupations des méthodologies de la sécurité qui considèrent que le cycle complet de la sécurité doit aussi intégrer les prescriptions relatives à un suivi du système pendant sa phase d'exploitation.

PROPOSITION D'UN MODELE CONCEPTUEL

INTRODUCTION

Quel que soit le système analysé, la Maîtrise des Risques s'intéresse aux résultats des comportements de celui-ci. L'approche analytique, effectue sur la base d'un ensemble de comportements déterminés, une analyse de tous les comportements dits à risque ou de toutes les conditions de sortie de cet ensemble. L'analyse structurelle va à établir les liens entre les objets et l'analyse de la dynamique identifier les enchaînements possibles d'événements et actions. A partir de cette approche un système ne se définit que par les conséquences de ses actions; ce qui est le postulat de départ de la conception par les spécifications. Les méthodes d'analyse correspondant alors aux méthodes de conception, c'est une des raisons qui font que pour palier ce mode commun dans la méthodologie, les analyses de sécurité sont réalisées par une équipe indépendante.

De même, l'approche analytique postule que le danger fait partie intégrante du système, sa reconnaissance se faisant à partir de la reconnaissance de certains signaux, objets ou relations. Ceci impliquant que sa détection ou visibilité relève plus de l'acuité de l'observateur, autrement dit de sa capacité ou de sa façon d'observer le système. Pour pallier ce problème, soit il faut chercher à épuiser le modèle en explorant toutes les combinaisons, soit chercher à reconnaître les signaux (base de données de connaissances). C'est le principe même de l'approche analytique du management des risques : connaissances des dangers puis connaissance du système observé, ou, observation d'un système donné à travers son propre système de connaissance, qui impose les limites que les outils et limites ne permettent pas de dépasser.

C'est pour répondre à cette problématique que nous allons dans ce chapitre aborder le paradigme *espaces-processus* fondateur de l'approche proposée dans ce mémoire. Après la présentation de ce paradigme nous aborderons les modèles associés. En premier lieu, sera présenté le modèle des espaces qui est le modèle de la perception par la propriété et en particulier son couplage au langage qui est un des éléments essentiel dans l'utilisation de cette approche. Ensuite, à travers l'espace des processus les deux dimensions de la dynamique, *instanciation* et *transformation*, seront abordées

PROPOSITION D'UNE APPROCHE ESPACES – PROCESSUS

Cette problématique fondamentale est liée à la capacité d'adaptation des systèmes complexes: des propriétés imprédictibles, non réductibles à la simple somme des acquisitions, peuvent apparaître. C'est-à-dire que la dynamique d'un système ne peut se décrire seulement par le fonctionnement de ses processus mais doit prendre en compte les transformations imposées par ses environnements. Si nous observons un système à un instant donné, alors il est possible d'observer des phénomènes qui se définissent par les objets, leurs propriétés, leurs relations mutuelles et les actions réalisées. Les objets, leurs propriétés et leurs relations définissent alors un espace qu'on qualifiera de favorable à l'exécution du projet d'action. Ce principe est la base de l'approche proposée, définie sous la forme d'un paradigme espaces – processus permettant de considérer un système non pas à travers une seule finalité mais comme la conjonction de tout ce qui est et peut être à l'origine d'une action. L'espace définissant l'ensemble des éléments sur lequel se construit l'action à venir, les processus étant les éléments définissant les actions ou intentions d'actions et permettant d'en déterminer les conséquences.

En considérant un projet d'action, on considère les objets, leurs propriétés et leurs relations qui définissent alors un espace favorable à l'exécution à ce projet d'action. Rappelons qu'en

modélisation systémique le concept de base n'est pas l'objet mais le concept général de processus définissant les changements qui affectent des objets, celui-ci étant alors défini comme une boite noire. Dans l'approche proposée nous allons refuser la matérialisation d'un objet qu'il soit structurel ou processus, pour ne s'intéresser qu'aux propriétés et à leurs évolutions. Chaque ensemble de propriétés et les relations reliant ces propriétés définiront un espace permettant l'action, c'est-à-dire la variation des états de ces propriétés. Le processus associé à l'action peut être exprimé par une combinaison d'états donnés et d'actions données conduite par et sur des objets donnés. C'est-à-dire que le processus est vu comme une somme de comportements partiels sur les états. Chaque comportement partiel peut éventuellement être défini par une suite ordonnée ou par une loi de comportement de la propriété. Ainsi la définition d'un projet d'action passe par la connaissance des propriétés et par la connaissance des comportements possibles de ces propriétés. Ainsi un système sera vu comme un espace de propriétés, et son comportement comme l'instanciation de cet espace.
Néanmoins seul l'aspect comportemental de la dynamique est défini ici. Pour formaliser la transformation il est nécessaire de faire appel à un autre principe important de la systémique qui est le principe d'entropie et en particulier d'irréversibilité : un système va toujours naturellement d'un état instable à un état stable et jamais l'inverse. Pour obtenir le passage de l'état stable à l'état instable, il est nécessaire de faire un apport au système. Cet apport devant remettre en cause la stabilité du système il doit affecter une propriété, une opération, ou une relation. Il peut être tentant de prendre en compte l'apparition d'objets supplémentaires; cependant, il ne faut pas oublier qu'en modélisation systémique l'objet n'a d'existence qu'à travers l'action et les changements qu'elle implique, c'est la raison pour laquelle les évolutions sont toujours données relativement aux propriétés et aux relations. A la différence du comportement qui peut se décrire par une succession d'instance d'un même espace, la transformation relève d'un apport, c'est-à-dire qu'elle prend son origine dans une relation qui modifiant ces espaces en produit un nouveau.

Ce principe fondamental n'établit pas uniquement le fait qu'un système est une collection de propriétés comportementales permettent la réalisation de certaines actions, mais, d'une part qu'une action potentiellement réalisable à un moment donné est à la fois lié à l'état courant mais aussi aux états passés de ces propriétés, et d'autre part, qu'une action va se réaliser pour répondre à une finalité qui n'est pas forcément immédiate. C'est le principe de la conjonction systémique qui propose « de tenir pour inséparable le fonctionnement et la transformation d'un phénomène, des environnements actifs dans lesquels il s'exerce et des projets par rapport auxquels il est identifiable » [LE MOIGNE 1990]. La dynamique d'un système ne peut se décrire seulement par le fonctionnement de ses processus mais doit prendre en compte les transformations imposées par ses environnements; si nous observons un système à un instant donné, alors il est possible d'observer des phénomènes qui se définissent par des propriétés, leurs relations mutuelles et les actions réalisées. Les propriétés et leurs relations définissent alors un espace qu'on qualifiera de favorable à l'exécution du projet d'action. .

Ce principe est la base de l'approche proposée définie sous la forme du paradigme espaces – processus permettant de considérer un système non pas à travers une seule finalité mais comme la conjonction de tout ce qui est et peut être à l'origine d'une l'action. L'espace définissant l'ensemble des éléments sur lequel se construit l'action à venir, les processus étant les éléments définissant les actions ou intentions d'actions et permettant d'en déterminer les conséquences.

Paradigme Espaces – processus : tout système peut se définir comme un projet d'action, c'est-à-dire comme une combinaison Espaces – Processus, les espaces contenant toutes les conditions et moyens nécessaires à l'achèvement du processus

Pour illustrer ce principe nous allons examiner deux exemple : le premier celui d'une pièce de théâtre qui nous permettra une représentation imagée de la notion d'espace et de processus, mais aussi la relation à l'environnement dans la finalité d'un système. Le second exemple, plus en

relation avec la finalité de la recherche sera basée sur un accident de tramway survenu il y a quelques années ; ce second exemple nous permettra d'illustrer l'importance du contexte et de l'environnement dans la transformation d'un système, aussi bien dans son comportement que dans sa finalité perçue.

La pièce de théâtre :

Une pièce de théâtre est a priori un système parfaitement déterminé dans les rôles et le scénario. Elle, est organisée en actes et en scènes construites sur la base d'une unité de temps, de lieu ou d'action. Chaque scène produit alors une transformation sur les propriétés des personnages. Il est alors facile de représenter l'histoire de la pièce de théâtre sous forme d'un enchaînement de processus qui à partir d'un espace donné produisent une transformation des objets ou des relations sur cet espace. Chaque transformation ou scène représentant une finalité d'action agissant comme des génératrices de sous espaces et chaque scène opérant une transformation ce sous espace et par extension sur l'espace général de l'acte et de la pièce. La pièce représente alors l'évolution globale d'un espace de départ subissant un ensemble de transformations discrètes et partielles, le spectateur assurant la continuité dans l'histoire. Quelque soit le jeu des acteurs et la mise en scène, l'histoire reste la même, la modification passagère de son texte par un acteur ne remettant pas en cause la pièce.

Or, et c'est ce qui présente le second intérêt, une pièce de théâtre n'est pas une simple histoire mais un divertissement qui requiert la collaboration d'un côté d'une histoire et d'acteurs et de l'autre d'un public. Prenons pour exemple la scène suivante: le retour du mari, l'amant étant bien sûr caché et essayons de déterminer son projet d'action: faire rire, créer du suspense, illustrer un drame de la vie courante ? La seule considération de la situation ne nous permet pas d'en tirer de conclusion. Le spectateur a dans son propre espace l'acquis que représentent les scènes précédentes, il a donc été prédisposé pour le rire, les larmes ou la tension. Mais attention même si la pièce est écrite et montée de façon à ce qu'une scène fasse rire, celle-ci peut provoquer d'autres réactions; en effet, le projet d'action de faire est défini par rapport à un public donné (identité socio culturelle), la même pièce face à une population différente produira peut être une pure indifférence, voire un jet de projectiles sur l'un ou l'autre des personnages.

Accident de tramway :

Cet exemple est directement inspiré de la collision par rattrapage entre deux rames de tramway survenue à Strasbourg le 28 octobre 1998. Pour bien comprendre cet exemple il faut savoir qu'en signalisation ferroviaire la voie est découpée en cantons sur lequel la présence d'un train est détectée en sécurité. Lorsqu'un canton est occupé, une signalisation lumineuse donne des ordres aux autres trains suiveurs de façon à ne jamais se retrouver dans une situation de collision. Ainsi les conducteurs de trains conduisent en respectant scrupuleusement les consignes de vitesse et la signalisation. Par contre, à la différence d'un train, le tramway est un véhicule urbain, c'est-à-dire que le conducteur applique le principe de la marche à vue ; ce qui se comprend lorsqu'on progresse au milieu de la circulation automobile ou piétonne. Cependant, par son caractère guidé, la conception des systèmes tramway reprend le principes de la signalisation ferroviaire pour les zones de manœuvre (pour éviter les mouvements d'aiguille intempestifs et éviter les conflits d'itinéraires) et dans certaines configurations où le conducteur du tramway n'a pas une visibilité suffisante pour surveiller la voie devant lui, ce qui était le cas à Strasbourg où la ligne présente une section courbe sans visibilité suffisante. Cette section a donc été protégée par un feu rouge signalant l'occupation de la zone suivante et devant être interprété comme un ordre d'arrêt. La particularité de cette zone est qu'elle inclut une station ; par conséquent, étant donné l'intervalle

séparant les tramways en exploitation, il arrive fréquemment qu'une rame soit en station lorsque la suiveuse arrive sur le feu d'occupation. Au fil du temps l'habitude est donc prise de franchir ce feu au rouge en adaptant la vitesse afin d'arriver en station lorsque la rame précédente dégage le quai, ce, jusqu'au jour où une rame est arrêtée dans la courbe…

Analysons maintenant cet accident : nous avons d'une part un système dont les propriétés à la conception respectent parfaitement les prescriptions. Ces prescriptions s'appuient sur un comportement d'objet opérant et sur une culture de signalisation ferroviaire. Nous avons, d'autre part, ce même système opéré dans le monde du tramway où la responsabilisation du conducteur peut conduire à des franchissements de rouge, autorisés. Nous constatons deux choses : primo que l'occurrence élevée d'une situation dont les conséquences sont nulles a dénaturé l'importance d'une information et autorisé un comportement a priori impossible lors de la conception du système, secundo que la répétition de ce comportement a finalement occulté le vrai sens du signal.

On peut considérer que le fonctionnement initial du système s'est transformé en présence d'un environnement actif (la mise en exploitation) et par rapport au projet auquel il était identifié (celui d'avertir de la présence d'une rame sur toute une zone, et non pas dans la seule station). Dans une démarche Espaces – Processus, l'espace initial (le système conçu et réalisé) s'est transformé par la mise en relation avec un autre espace, celui des conducteurs et a acquis une capacité d'adaptation qui a modifié ses propriétés (l'importance du signal).

Mais attention, cette transformation du comportement n'est pas forcément inconsciente. Dans notre exemple, le conducteur de la rame arrêtée prévoyant la collision avec la rame suiveuse, a rassemblé tous les passagers vers l'avant ce qui a limité les conséquences de l'accident.

Pour bien fixer la différence avec la dynamique du comportement, imaginons que le tramway soit sorti de la voie pour une raison quelconque, alors nous serions dans le cas d'une instanciation de l'espace du système car en aucun cas une propriété n'aurait été modifiée ; nous serions simplement dans le cas d'un état particulier de cette propriété.

Si nous revenons maintenant sur la définition du paradigme nous constatons que ce qui caractérise un espace n'a pas encore été défini. Il serait tentant pour décrire les espaces de se référer à des notions comme l'objet ou la dimension qui caractérisent des relations représentant des unités ou communauté d'objets en utilisant des concepts comme les unités physiques (objet ou lieu), de temps, d'action, d'organisation ou même d'objectif. En effectuant ce raccourci, qu'a priori rien ne dément puisqu'il apparaît évident que ces unités définissent des espaces, nous induirions alors un biais par l'intermédiaire d'une vision structurelle ou organisatrice du système. Mais surtout, nous limiterions les relations génératrices d'un espace à ces seules dimensions, ce qui écarterait les communautés d'objets par les propriétés ou les opérations qui peuvent être à la source de phénomènes de redondance structurale ou fonctionnelle ; sensibles en particulier dans les rapports du système à l'environnement.

PROPOSITION D'UN MODELE DES ESPACES

Espaces

A travers la définition du paradigme espaces – processus nous avons identifié sans les définir les deux premiers concepts fondateurs de l'approche proposée. Dans un premier temps, définissons ce qui constitue un espace. Etant donné que la conceptualisation est une forme particulière de perception, il serait naturel de penser que, quelque soit la façon dont on l'aborde, la vision que nous offre un système à un moment donné est celle d'objets. L'objet serait alors l'unité

atomique des espaces ; mais peut-on identifier un projet d'action ou même une action à un objet ? Imaginons de nous réveiller à bord d'un véhicule. Avant même d'ouvrir les yeux nous avons identifié, au moins partiellement, l'espace dans lequel nous nous trouvons par les accélérations, la dureté (ou le moelleux pour les chanceux) d'un siège, etc. Nous percevons l'espace non pas par l'objet mais par ses propriétés ; de même, nous identifions une action en cours par des propriétés.

Un espace est un ensemble de propriétés favorables à l'achèvement d'un projet d'action particulier. L'unité atomique de l'espace est la propriété.

Il faut noter que même une approche analytique tente de dégager les propriétés d'un système par l'identification de fonctions et la caractérisation des organes par les spécifications.

Propriétés

La propriété est l'abstraction de ce par quoi on perçoit la chose observée. L'abstraction est une démarche intellectuelle qui consiste à concentrer la perception qu'on a d'un objet sur un élément représentatif; c'est-à-dire que la vision qu'un modélisateur a d'un objet est celle de propriétés ou de comportements qu'il pourra abstraire en caractéristiques passives :les attributs, ou actives : les opérations. L'objet en tant qu'unité sémantique représente l'ensemble de ses images mais aussi l'ensemble de ses comportements. Cette notion d'unité sémantique est très proche de la notion de langage. Cette notion de langage représente le lien fondamental entre la vision du réel et le concept manipulé et d'autre part les éléments de communication entre objets d'un même modèle. Ceci car à la notion de langage est associée la notion d'information portée par un terme de ce langage. Cette information intègre un typage du terme, c'est-à-dire le sens qui lui est attribué, et une valeur du terme, c'est-à-dire l'état ou la position de l'information sur un domaine de définition. Par exemple, un signal R11, plus connu sous le terme de feu routier :

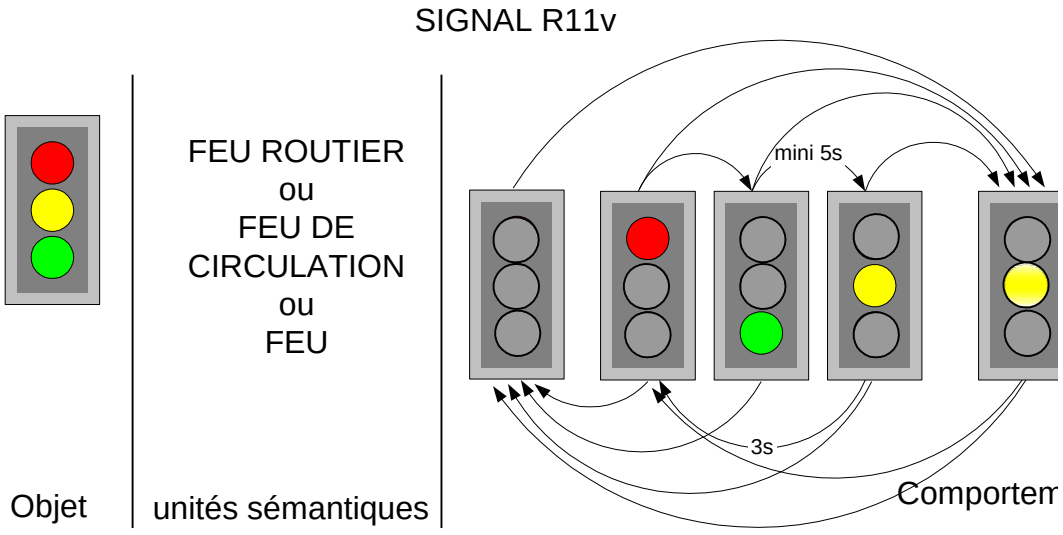


Figure 28 : Conceptualisation et perception

Dans le modèle proposé, la propriété seule nous intéressant, se définit par une unité sémantique (mot représentatif) et par un domaine de définition.

Le domaine de définition est constitué des différents états ou instances de la propriété, par exemple : bleu, blanc, rouge. L'unité sémantique est le mot ou l'expression par lequel on nomme la propriété : couleur, forme, trajectoire,etc.

Le langage au sens d'information, n'est dans l'absolue qu'une représentation d'une réalité perçue; c'est-à-dire que les risques associé au langage sont liés à la compréhension et à l'interprétation des termes. En effet, étant donné que l'information liée à un terme est un vecteur (sens, état), il existe un phénomène de polymorphisme sur les termes. Par exemple, la position d'un avion sur l'espace aérien est dans l'absolu est un vecteur (x, y, z). Par contre, pour le pilote ou le contrôleur, cette position sera donnée relativement à un repère pré établi avec une terminologie codée ; Novembre1, Echo2 par exemple, pour des positions particulières autour d'une tour de contrôle, ou à un niveau de vol qui ne correspond pas directement à l'altitude vraie mais à un référentiel altimétrique préétabli, unique et commun à tous les avions. Nous avons donc pour un même terme représentant une même propriété, deux expressions différentes. De même le langage peut définir aussi bien une information d'état, qu'une information d'action, avec le même problème de polymorphisme. Nous verrons dans la suite de ce mémoire que le modèle de représentation d'une propriété doit intégrer un nommage propre au modèle auquel on associe le couple domaine de définition, unité sémantique.

Toute la description de l'espace s'appuie sur la représentation des objets et des relations à partir d'espaces de propriétés. Le concept de propriété est l'unité atomique de l'espace observé et peut aussi bien représenter une propriété au sens de l'aspect que du comportement. Le concept de propriété est donc fondateur du paradigme espaces- processus car il permet à la fois une description de l'espace mais aussi une description de comportements indépendants de la dynamique d'un système donné; ce concept autorise à la fois une manipulation de l'espace généralisé et de l'espace particularisé (instancié, environné).

L'objet en tant que chose physique ou système existe mais il est alors espace de propriétés. En effet, tout objet quelconque est perceptible par son état (ensemble de ses propriétés à un instant donné) et son comportement (ensemble de ses actions). Or, dans une approche systémique nous nous intéressons au projet d'action, c'est-à-dire que nous allons intellectuellement isoler une organisation à partir des propriétés et des comportements de l'objet que nous associons à un projet, c'est l'espace de ce projet. Si nous nous intéressons à ce seul projet d'action nous pouvons ignorer les propriétés et comportements restants; par contre, si nous intéressons à d'autres projets d'actions auquel participe l'objet, nous obtiendrons alors d'autres espaces. Toutefois, il est évident que ces espaces ne sont pas indépendants les uns des autres, ils sont associés par le fait de mettre en jeu le même objet, ils sont en relation.

Relations

Le concept de relation se retrouve largement dans la définition de l'approche systémique qui convient que les parties se définissent et existent par leurs relations mutuelles et non par ce qu'elles sont. La relation formalise un lien particulier qui relie plusieurs propriétés. Une relation peut caractériser plusieurs formes de liens : généricité, partage, dépendance, influence, association.

De même que la propriété, la relation possède une unité sémantique et un domaine de définition. Par contre, le domaine de définition d'une relation ne décrit pas les caractéristiques intrinsèques d'une propriété mais les caractéristiques permettant d'établir un lien entre plusieurs propriétés. La relation est une propriété d'espace car elle décrit une communauté entre propriétés ;

la relation est une notion constructrice d'espace. Le fait d'établir une relation d'association de propriétés est déjà en soi identifier une organisation. Nous admettons facilement que le projet d'action n'est pas la seule relation constructrice d'espace, par contre, toute construction d'espace, et par extension toute relation, définit potentiellement un projet d'action.

L'espace général

Avec les deux concepts de propriétés et de relation nous avons défini les éléments descriptifs constitutifs du modèle des espaces. Néanmoins, si la vision des espaces par les propriétés ne limite pas une démarche descendante du global au particulier, elle ne doit pas non plus limiter une démarche inverse. C'est-à-dire, tout système représenté sous la forme d'un modèle des espaces devra admettre une espace plus large, correspondant à une perception plus large de la réalité observée.

Il ne peut être question de définir de façon exhaustive un espace représentant le monde réel. La modélisation s'effectue dans un cadre particulier d'observation et d'évaluation, il n'est donc pas nécessaire de chercher à tout identifier et à tout représenter. Il est plus approprié de considérer un espace ouvert, qu'on appellera espace général. L'espace réel se définissant comme un ensemble non limité d'entités, de matières, énergies, d'informations ou même d'idées et d'actions, l'espace général se définira comme le rassemblement de propriétés, de relations, et d'espaces.

La notion d'espace général doit être appréhendé comme la globalité de l'espace observable qui est appelé espace général et non espace réel pour éviter qu'il ne subsiste aucune ambiguïté entre la réalité observée et ce qui est observable.

LA DYNAMIQUE DES ESPACES : LES PROCESSUS

L'instanciation : première dimension de la dynamique des espaces

L'ensemble des recherches sur la dynamique des systèmes, et en particulier les travaux sur la systémique, montrent que la dynamique d'un phénomène s'exprime d'une façon complexe d'une part par le comportement - les différentes formes de réalisation ou instanciation des propriétés des objets considérés - et d'autre part par l'émergence de nouvelles propriétés, c'est la transformation ou évolution. Nous avons donc l'expression d'une dynamique complexe : instanciation – transformation. Le comportement décrit les changements d'état d'une propriété sur son domaine de définition. Chaque état de la propriété représente alors une instanciation de cette propriété. L'instanciation, telle que définie, possède une propriété fondamentale pour la suite des travaux de modélisation, qui est la propriété d'endomorphisme. Les différents intérêts de cette définition et de sa propriété vont être décrit ici et démontrés avec le modèle de représentation proposé. La première conséquence de cette propriété est que l'instanciation n'est pas une propriété ou une relation particulière sur un espace. En effet, l'instanciation ne construit pas un espace d'évolution de la propriété mais une représentation de la trace des évolutions de cette propriété. C'est-à-dire que rien ne permet d'affirmer que la réunion des comportements de deux propriétés distinctes décrivent un espace; seule une relation permettra de déduire une instance sur une propriété en fonction d'une instance sur autre propriété et réciproquement. L'instanciation est un phénomène endomorphe.

La propriété d'endomorphisme de l'instanciation est aussi capitale pour la conceptualisation d'un système car elle permet à n'importe quel observateur de décrire la chose perçue depuis son point de vue ; le point de vue du système ne s'impose que lorsqu'on considère son comportement.

En effet, même si la vision retranscrite du système est celle que d'autres systèmes ont sur lui, l'analyse du comportement sera toujours effectuée vis-à-vis de ce système sur lui-même. Enfin, il est devient possible de considérer le comportement conjoint de système indépendants en limitant l'impact de la distorsion sur les interfaces. En effet, la liaison entre comportements de systèmes disjoints ne peut se faire à partir de leurs instances mais qu'à partir de l'observation des relations existant entre leurs propriétés et non à travers les propriétés intrinsèques des systèmes observés. En substance, la propriété d'endomorphisme de l'instanciation implique que le comportement et l'espace de propriétés sont deux concepts de représentation bornés.

On peut alors affirmer que l'instanciation crée une dimension commune non pas à des espaces mais à des comportements sous forme de partitions des états de l'espace. L'instanciation dimensionne la dynamique du comportement d'un espace à partir son origine (état initial); c'est-à-dire que du concept défini par des propriétés (attributs et opérations), l'instanciation crée une réalisation de ce concept munie d'un état et d'un comportement, qu'on appelle un objet ou système. De même cette propriété est importante dans la démarche de raffinement. En effet, si on décide de raffiner la description d'une propriété, toute décomposition supplémentaire de cette propriété respectera l'instanciation du niveau supérieur. C'est à dire que la décomposition d'une propriété ne peut être se faire qu'à partir d'une spécialisation, et, inversement toute généralisation d'un comportement décrira un sous espace des propriétés de niveau inférieur.

Nota : on retrouve là une caractéristique essentielle des systèmes de sécurité, à savoir que leur comportement doit être parfaitement prédictible, c'est à dire que leur espace de comportement doit être parfaitement maîtrisé. Ainsi en sécurité une bonne conception n'est valable que sur un environnement identifié pour une finalité donnée. A contrario, la transformation n'étant pas prise en compte celle-ci doit donc évitée en exploitation.

La transformation : seconde dimension de la dynamique des espaces

La grande majorité des auteurs insistent sur le fait que, pour un système évolué, la stabilité n'est que dans la finalisation. Un système évolué est par définition un système capable d'auto organisation afin d'achever un objectif donné. Dans ce cas, la poursuite de l'objectif et assurée non pas par une évolution des propriétés descriptives du système mais par une évolution de leur organisation. L'organisation des propriétés étant établie à partir des relations, c'est donc l'évolution de celles-ci qui peut modifier ou faire émerger de nouvelles propriétés. Cependant la transformation considérée sous ce seul point de vue ne prend en compte que les capacités d'auto adaptation d'un système.

Pour fournir une définition ouverte de la transformation il faut revenir au principe d'entropie de la systémique et en particulier au principe d'irréversibilité. Ce principe postule qu'un système va toujours vers un état de stabilité et jamais l'inverse. Pour obtenir un passage de l'état stable vers un état instable il est nécessaire de faire un apport au système. D'après la définition que nous avons fourni d'un système, c'est-à-dire celle d'un espace de propriétés et de relations, cet apport doit soit :

- affecter une propriété ou une relation existante : unité sémantique ou domaine de définition,
- consister en l'apport d'une nouvelle propriété ou relation.

Néanmoins, le fait d'apporter une nouvelle propriété à un espace ne se traduit pas forcément par une transformation de celui-ci vis-à-vis des projets d'action par lesquels il se définit ; il est nécessaire que la propriété apportée établisse de nouvelles relations avec les

propriétés initiales. On retrouve le postulat décrit précédemment qui affirme que la transformation n'est pas le produit d'une simple évolution des caractéristiques mais le produit d'un changement de l'organisation, donc des relations. Bien sûr, il n'est en aucun cas exclu que le système à nouveau stabilisé n'ai pas certaines de ses propriétés transformées.

On a donc une approche de la transformation plus large que la simple capacité d'auto adaptation d'un système. La transformation est une notion complémentaire de la dynamique du comportement. En effet, l'instanciation est un phénomène endomorphe qui décrit les successions d'état que peut prendre une propriété, alors que la transformation est un phénomène exomorphe et irréversible qui décrit un nouvel espace. Il est important de noter qu'une fois la transformation effectuée, la propriété d'endomorphisme de l'instanciation conduit à un nouveau système stable.

Une des conséquences immédiates de l'expression de cette dynamique complexe va se retrouver dans la capacité d'évolution du modèle soit par les changements survenant dans son environnement soit en prenant en compte les différentes étapes du cycle de vie d'un système à travers ses propriétés. Par exemple, la formation, va correspondre à l'adjonction de propriétés au domaine de connaissance global du système mais aussi des opérateurs humains. Il sera alors possible de modéliser le système de connaissance comme un ensemble de propriétés dont la mise en relation avec le système va transformer le système, et ainsi d'évaluer l'impact de telle ou telle formation.

Par contre, un des effets de la transformation doit être pris en compte dans la modélisation pour conserver au modèle sa capacité à être affiné par morceau ; en effet, chaque modification d'une propriété d'un espace, de manière chaque apport que va représenter un complément d'analyse ou de connaissance va créer un nouveau système qui va se stabiliser à nouveau. Pour être robuste, le modèle du système devra alors définir un espace sur lequel les évolutions du modèle lui-même restent endomorphes. Nous verrons dans un chapitre suivant de ce mémoire comment la définition d'un modèle de système général permet de prendre en compte cet aspect de mise en relation d'espaces à finalités différentes.

CONCLUSION

Tout ce qui a été écrit dans ce chapitre peut se résumer ainsi :

- Il est permis de conceptualiser un objet ou un système de manière générale comme un espace favorable à un projet d'action.
- Il est permis de conceptualiser les objets par leur propriétés, le concept de propriété portant unité sémantique (sens) et domaine de définition (les différents états que peut avoir la propriété).
- Il est permis de conceptualiser l'organisation des objets par les relations s'établissant entre les propriétés, le concept de relation portant unité sémantique et domaine de définition (caractéristiques du lien). La relation est assimilable à une propriété d'espace.
- Il est permis de conceptualiser la dynamique d'un système sous une forme complexe instanciation – transformation.
- Le concept d'instanciation décrit la dynamique du comportement d'une propriété, c'est-à-dire les suites d'états que peut prendre cette propriété.
- Le concept de transformation décrit la dynamique de la mise en relation de propriétés, c'est-à-dire l'évolution de l'espace contenant ces propriétés lors de leur mise en relation.
- Le concept de processus est l'expression particulière de la dynamique instanciation – transformation associé à un espace de départ et à un objectif donné.

De manière générale le processus décrit les comportements et évolutions d'un système dans le but d'achever un objectif donné. Mais un processus peut aussi décrire la somme des

comportements et évolutions qui ont conduit à un résultat donné. Le processus est bien l'expression d'une dynamique complexe instanciation – transformation relative à un projet d'action. Cependant, la notion de processus est une vision réductrice de la dynamique car la transformation étant irréversible le processus est alors perçu comme une suite ordonnée. Ainsi il est aisé de percevoir un système à partir soit d'un espace et d'une suite de transformations - comportements, soit d'un espace et d'une suite de transformation aboutissant à un espace favorable à un comportement donné.

Cette perception d'un système et de sa dynamique à partir des seuls processus peut conduire à une analyse incomplète : en ne considérant que les processus on oublie la notion de système comme espace favorable à un projet d'action, en particulier favorable à des projets d'actions indésirables. C'est la raison pour laquelle espaces et processus sont indissociables dans l'approche proposée.

PROPOSITION D'UN MODELE DE REPRESENTATION

INTRODUCTION

Le chapitre précédent présente l'effort initial d'identification et de définition de la sémantique des concepts fondamentaux d'un modèle conceptuel systémique. Ces concepts sont les unités de base, ou si l'on veut parler de construction, les briques de base, autorisant la conceptualisation puis la modélisation d'un système et de sa dynamique.

L'objectif premier d'un modèle systémique n'est pas de représenter un système par sa structure mais de s'attacher à l'action et à son évolution. Une transformation d'objets réels en objets conceptuels correspond à une simple approche analytique. Le modèle de représentation adopté doit éviter autant que possible de retranscrire l'interprétation de telle ou telle structure perceptible pour rester concentrer sur la représentation du phénomène observé.

Pour être acceptable le modèle de représentation doit comporter les moyens de répondre à une analyse critique; c'est-à-dire qu'il ne doit pas être nécessaire de consulter son modélisateur pour justifier les résultats. Ces contraintes de formalisation se traduisent par les qualités que doit avoir le modèle de représentation, à savoir : lisibilité, fiabilité, neutralité, confiance dans la représentation choisie mais aussi décidabilité sur le résultat.

Le modèle de représentation décrit dans ce chapitre va à partir d'une représentation unifiée de la propriété et de l'objet espace de propriété proposer une représentation des comportements et de leur dynamique sous forme d'expressions permettant un couplage fort avec le langage aussi bien dans la modélisation que dans la communication entre les objets du modèle. Nous allons d'abord donner une définition particulière de la propriété, reliée à sa représentation sémantique (représentation dans le langage). Nous allons ensuite, montrer comment une description des relations entre ces propriétés, et en particulier des relations comportementales, définissent des expressions rationnelles. Une forme algébrique permettant une manipulation plus conviviale des expressions rationnelles sera proposée. Enfin, nous aborderons la manipulation des expressions pour décrire les relations ou l'instanciation.

PROPRIETES, OBJETS ET ESPACES: DEFINITION UNIFIEE

L'objet n'a pas d'intérêt au sens physique mais est vu à travers ses propriétés.

On défini p[P, $\mathscr{P}$] comme la notation d'une propriété avec :

- l'identifiant p. Dans le cas d'une propriété simple, par exemple un attribut unique (couleur verte), p représente alors une valeur; dans le cas d'une propriété dynamique, par exemple la couleur prise parmi rouge, vert, jaune, p représente une variable

- le domaine de définition P qui défini un espace représentant l'ensemble des états de la propriété, mais aussi les conditions nécessaires aux changements d'états. Le domaine de définition de la propriété défini donc un espace de réalisation de la propriété. La réalisation couvre valeurs, états ou exécution d'opérations appartenant au domaine de définition. Le concept de propriété peut aussi bien représenter une propriété au sens de l'aspect que du comportement.

- l'unité sémantique $\mathscr{P}$ est l'élément de langage (mot ou terme) qui représente le concept. L'unité sémantique représente l'élément de couplage entre la manipulation intellectuelle de l'information et sa manipulation dans le modèle. La propriété est un couple formé d'une unité sémantique représentant la propriété et un domaine de définition de cette propriété. Cette propriété peut être passive, un attribut ou active une opération. A travers la même notation nous allons

pouvoir représenter une propriété simple, exemple vert[{vert},"vert"], une propriété dynamique, exemple couleur[{vert, jaune, rouge},"couleur"].

De manière générale, l'identifiant utilisé seul indique que nous nous intéressons à l'instance de la propriété. Cette instance pouvant être une valeur ou une variable nous adopterons la convention suivante :

- p indique que nous utilisons la variable,
- p_{indice} indique que nous utilisons une valeur ou une instance.

Nous avons ainsi établi une représentation généralisée unique pour la propriété et l'espace. Seule exception l'espace général, qui représente à la fois les propriétés, les unités sémantiques et les instances qui devrait être noté $\omega[\Omega,$"espace général"] mais que nous choisissons de noter simplement Ω étant donné que nous ne nous intéresserons pas à ses états particuliers.

Ces définitions et les conventions de notation établies sont la représentation unifiée de l'élément fondamental de l'approche espaces – processus, à savoir la propriété.

LANGAGE ET EXPRESSIONS RATIONNELLES DE PROPRIETES

Introduction

Nous venons de définir une notation des propriétés incluant une représentation sémantique, associée à la notion de langage. Cette association représente d'une part le lien fondamental entre la vision du réel et le concept manipulé et d'autre part les éléments de communication entre objets d'un modèle. Si cette définition permet de décrire chaque espace de propriété, elle ne permet pas d'exprimer les relations qui existent entre ces propriétés. En particulier, cette représentation est insuffisante pour décrire les relations entre différentes instances de propriétés, relations qui définissent un comportement.

Nous allons établir un modèle de représentation permettant de retranscrire le plus directement possible les expressions sémantiques, et pour cela, nous allons montrer que chaque espace, formé de propriétés et de relations, peut se définir comme une expression rationnelle sur l'espace général Ω.

Définition des opérateurs d'expressions

Par définition, une partie d'un ensemble est dite rationnelle si elle peut être obtenue à partir d'expressions rationnelles de ses parties finies. Toute partie finie étant une réunion finie d'ensembles à un élément, il est donc nécessaire de définir les opérateurs de ces parties finies nous permettant de décrire les attributs et les comportements d'un objet à partir de ses propriétés élémentaires.

Elément neutre sur Ω :

Définissons tout d'abord l'élément neutre par la propriété particulière $\in[\varnothing,\in]$. Cet élément neutre n'est pas nécessairement une propriété dont le domaine de définion est vide ou une expression vide, il représente une propriété existante mais dont l'absence de relation vis-à-vis d'un projet d'action la rend neutre ; elle est alors représentée par la propriété $\in[\varnothing,\in]$.

Nous reviendrons ultérieurement sur l'importance et la signification de cet élément neutre qui n'est pas un simple artifice de démonstration.

Premier opérateur : somme de propriétés ou union de propriétés noté "+" :

Soient p[P,$\mathscr{P}$] et q[Q,$\mathscr{Q}$] deux propriétés de Ω, alors l'association des instances de ces propriétés est défini par :

p[P,$\mathscr{P}$] + q[Q,$\mathscr{Q}$] = (p + q)[P ∪ Q, ($\mathscr{P}$et $\mathscr{Q}$)] et

p[P,$\mathscr{P}$] + ϵ[∅,ϵ] = (p +ϵ)[P ∪ ∅, ($\mathscr{P}$et ϵ)] = p[P,$\mathscr{P}$]

Etant donné que ∪ est commutative et associative on constate facilement que "+" est une opération commutative et associative.

L'opérateur "+" vérifie la propriété d'endomorphisme de l'instanciation. Quelque soit x_i une réalisation de x[X,$\mathscr{X}$], par définition $x_i \in X$ et quelque soit y_i une réalisation de y[Y,$\mathscr{Y}$], par définition $y_i \in Y$. Il vient donc naturellement que la somme de domaine de réalisation est l'union des domaines de définition des propriétés.

L'association d'instances de propriétés définit non pas une nouvelle propriété mais un nouvel espace de réalisations qui est l'union des espaces de réalisations de ces propriétés.

On constate alors que (Ω, +, ϵ[∅,ϵ]) constitue un monoïde libre commutatif de l'espace général Ω, c'est-à-dire que le domaine de définition d'une propriété étant son propre espace de réalisation, l'espace de réalisation d'un espace de propriétés s'écrira comme la somme des espaces de réalisation de ses propriétés.

Nota : une propriété n'a pas de symétrique pour +, (Ω, +, ϵ[∅,ϵ]]) n'est pas un groupe.

Second opérateur : l'opérateur de relation entre propriétés noté "."

Soient p[P,$\mathscr{P}$] et q[Q,$\mathscr{Q}$] deux propriétés de Ω, alors une relation entre ces propriétés est défini par :

p[P,$\mathscr{P}$] . q[Q,$\mathscr{Q}$] = (p.q)[P×Q ={ $p_i.q_i$ | $p_i \in P$, $q_i \in Q$ }, ($\mathscr{P}$en relation avec $\mathscr{Q}$)] et

p[P,$\mathscr{P}$] + ϵ[∅,ϵ] = (p.ϵ)[P×∅, ($\mathscr{P}$en relation avec ϵ)] = p[P,$\mathscr{P}$]

L'opérateur "." définit la relation au sens le plus large. Il ne définit pas la nature de la relation, mais traduit qu'il existe un lien entre deux propriétés, qu'elles évoluent *ensemble*.

On constate alors que (Ω, . , ϵ[∅,ϵ]) constitue également un monoïde libre de Ω, c'est-à-dire que l'espace de réalisation de deux espaces de propriété en relation s'écrira comme le produit des espaces de réalisation de ces propriétés.

En revanche, l'opérateur de relation n'est pas commutatif. En effet, Soient p[P,$\mathscr{P}$] et q[Q,$\mathscr{Q}$] deux propriétés de Ω, alors p.q signifie qu'une instanciation de p implique une instanciation de q, mais pas forcément qu'une instanciation de q implique une instanciation de p.

Un exemple suffit à le montrer, prenons une de ces lampes qui peuvent diffuser plusieurs couleurs; si l'association des propriétés rouge.allumée est vraie elle n'implique pas forcément allumée.rouge.

Opérateur d'itération "*"

Soit alors l'opérateur "*" d'itération sur l'espace général Ω, tel que Ω^* désigne l'ensemble des parties de Ω définie par Ω^0 = ϵ[∅,ϵ], Ω^1= Ω et $\Omega^n = \Omega.\Omega^{n-1}$

Soit E un espace quelconque de Ω^*, alors E^0= ϵ[∅,ϵ], E^1= E, $E^n = E.E^{n-1}$ et $E^* = \bigvee_{i\geq 0} E^i$

Pour une propriété p[P, $\mathcal{P}$] de E, $P^* = e+p_0+\ldots+p_n+ \sum_{i=0}^{i=n} p_{i.}.(p_{i+1} + ... + p_n)$

Cette définition des opérateurs +, . et *, ainsi que de l'élément neutre ∈[∅,∈], nous permet d'exprimer

- que chaque partie de l'espace général Ω est une expression rationnelle sur (Ω, +, . , *, ∈),
- quelle que soit p[P, $\mathcal{P}$] propriété de Ω, une instance p_i de p[P, $\mathcal{P}$] est une expression rationnelle, P est une expression rationnelle, P^* est une expression rationnelle.
- quelle que soit p[P, $\mathcal{P}$] de Ω et quelle que soit q[Q, $\mathcal{Q}$] de Ω, p[P, $\mathcal{P}$].q[Q, $\mathcal{Q}$] et p[P, $\mathcal{P}$] + q[Q, $\mathcal{Q}$] sont des expressions rationnelles sur Ω.
- quelle que soit p[P, $\mathcal{P}$] de Ω et quelle que soit q[Q, $\mathcal{Q}$] de Ω, $P^*+Q^* = (P+Q)^*$ et $P^*.Q^* = (P.Q)^*$

En d'autres termes, n'importe quel objet de l'espace est une expression rationnelle de ses parties finies, celles-ci étant représentées par des propriétés élémentaires, des associations de ces propriétés, et par l'union de leurs espaces de réalisation.

La conséquence en est qu'il est possible de définir n'importe quel comportement comme la somme d'expression rationnelles de propriétés; une expression rationnelle étant une suite de symboles, les propriétés sont l'alphabet de Ω, et les espaces de propriété sont les parties de Ω.

Propriétés :

a) Le domaine de définition d'une propriété étant la somme de toutes ses réalisations, tout objet étant défini par la relation de deux propriétés il est possible de définir un majorant de l'espace de réalisation de cet objet comme le produit des deux domaines de définition des propriétés. En d'autres termes, soit p[P, $\mathcal{P}$] et q[Q, $\mathcal{Q}$] deux propriétés de Ω, alors le domaine de définition de l'objet défini par l'association de ces deux propriétés est défini sur $P^*.Q^*$; c'est à dire qu'il est possible de définir n'importe quel objet comme une expression rationnelle sur les domaines de définition des propriétés sur Ω à partir des opérations union, relation et itération. Chaque instance d'une propriété étant elle-même une propriété élémentaire (singleton), il est possible de définir le domaine de définition à partir des expressions rationnelles des propriétés élémentaires le composant.

b) L'opérateur de relation "." est distributif par rapport à l'opérateur "+".

Considérons trois propriétés p[P, $\mathcal{P}$], q[Q, $\mathcal{Q}$] et s[S, $\mathcal{S}$].

Alors d'après la définition des opérateurs "." et "+"

(p[P, $\mathcal{P}$] + q[Q, $\mathcal{Q}$]). s[S, $\mathcal{S}$] =(p+q).s[(P∪Q) ×S, ($\mathcal{P}$et $\mathcal{Q}$ en relation avec $\mathcal{S}$].

C'est-à-dire que le domaine de définition de la propriété résultant de cette relation sera défini sur :

$(P\cup Q) \times S = \{x_i.s_i \mid x_i \in P\cup Q, s_i \in S\}$

$= \{x_i.s_i \mid x_i \in P, s_i \in S\} \cup \{x_i.s_i \mid x_i \in Q, s_i \in S\}$

$= P\times S \cup Q\times S$

Ce qui vérifie (p[P, $\mathcal{P}$] + q[Q, $\mathcal{Q}$]). s[S, $\mathcal{S}$] = p[P, $\mathcal{P}$] . s[S, $\mathcal{S}$] + q[Q, $\mathcal{Q}$]). s[S, $\mathcal{S}$]

c) en remarquant que les propriétés élémentaires sont des singletons de la forme a[{a},"a"] (par exemple vert[{vert},"vert"], il est possible d'utiliser une notation simplifiée des expressions rationnelles que nous adopterons par la suite.

Soient p[P, $\mathcal{I}$] et q[Q, $\mathcal{A}$] deux propriétés de Ω, on notera :

- p_i+q_j la somme de deux instances particulières de p[P, $\mathcal{I}$] et q[Q, $\mathcal{A}$],
- p+q la somme de deux instances quelconques de p[P, $\mathcal{I}$] et q[Q, $\mathcal{A}$],
- P+Q la somme (ou union) des deux espaces de réalisation de p[P, $\mathcal{I}$] et q[Q, $\mathcal{A}$],
- p_i+Q la somme d'une instance particulière de p[P, $\mathcal{I}$] avec l'espace de réalisation de q[Q, $\mathcal{A}$],
- p+Q la somme d'une instance quelconque de p[P, $\mathcal{I}$] avec l'espace de réalisation de q[Q, $\mathcal{A}$],
- $p_i.q_i$ la relation de deux instances particulières de p[P, $\mathcal{I}$] et q[Q, $\mathcal{A}$],
- p.q la relation de deux instances quelconques de p[P, $\mathcal{I}$] et q[Q, $\mathcal{A}$],
- p_i.Q la relation d'une instance particulière de p[P, $\mathcal{I}$] avec la propriété q[Q, $\mathcal{A}$],
- p.Q la relation d'une instance quelconque de p[P, $\mathcal{I}$] avec la propriété q[Q, $\mathcal{A}$],
- P.Q la relation des domaines de définition de p[P, $\mathcal{I}$] et q[Q, $\mathcal{A}$]
- P^* l'ensemble des expressions rationnelles décrivant la propriété p[P, $\mathcal{I}$].

On remarque aussi que si l'opérateur de relation définit sans ambiguïté un objet ou espace de propriétés, la somme définit une propriété ou un objet sous forme d'un espace de réalisation et par conséquent le comportement d'une association de propriétés (un système) comme la mise en relation de ces espaces de réalisation.

L'ensemble P^* des expressions rationnelles de cet espace représente un ensemble fini des instanciations qui va être modifié par l'introduction d'une nouvelle propriété ou d'une nouvelle relation, il y a alors transformation.

Exemple applicatif

Voyons maintenant à travers un exemple concret l'intérêt et l'application de ces expressions rationnelles et surtout comment les utiliser.

Comme exemple applicatif, reprenons notre feu routier décrit au chapitre précédent dont la figure illustrant le fonctionnement est répétée ci-dessous :

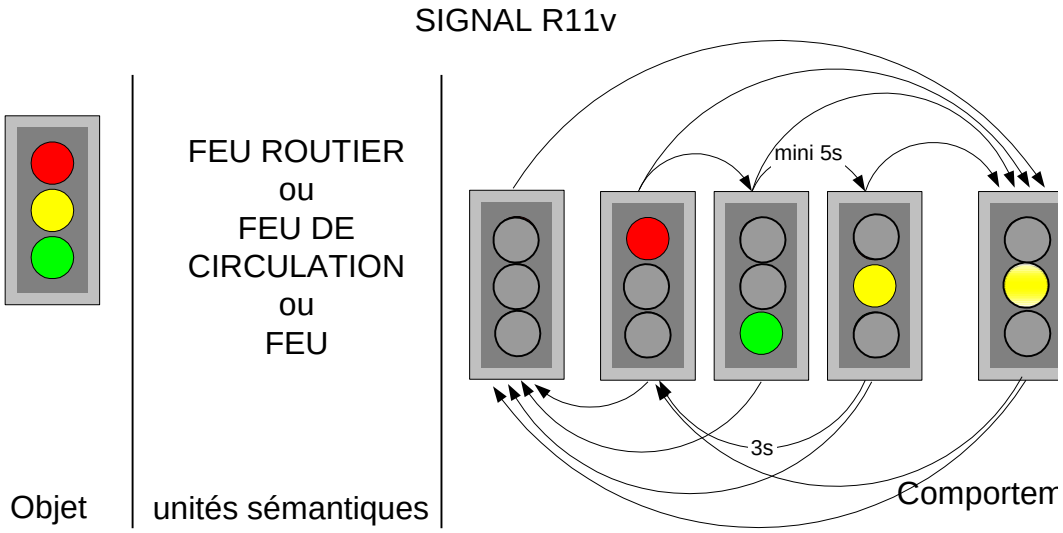


Figure 29 : Feu routier R11v

La première question est comment appliquer les concepts que nous venons de développer sur nos observations.

Expression de la propriété :

A partir de la seule observation du feu routier, nous pouvons alors identifier les propriétés suivantes :

- les propriétés élémentaires vert[{vert}, "vert"], jaune[{jaune},"orange"], rouge[{rouge}," rouge"] qui donnent une propriété couleur[{vert , jaune, rouge},"couleur"],
- les propriétés éteint[{éteint},"éteint"], fixe[{fixe},"allumé fixe"], clignotant[{clignotant},"allumé clignotant"].

Nous constatons que nous avons pu décrire les différentes propriétés caractérisant les états du feu sous forme de propriétés élémentaires ou d'un niveau supérieur (couleur).

L'opérateur de relation "."

L'expression du domaine de définition du comportement attendu du feu routier. Celui-ci peut se décrire textuellement par :

"toutes couleurs éteintes, ou (en séquence (rouge allumé (sous entendu vert et jaune éteints), puis vert allumé puis jaune allumé)) ou jaune clignotant".

Cette petite phrase est en fait une expression rationnelle :

(couleur.éteint) +
(((vert.éteint).(jaune.éteint).(rouge.allumé)).((vert.allumé).(jaune.éteint).(rouge.éteint)).((vert.éteint).(jaune.allumé).(rouge.éteint)).((vert.éteint).(jaune.éteint).(rouge.allumé))) +
((rouge.éteint).(vert.éteint).(jaune.clignotant))

Pour écrire cette seule expression rationnelle nous avons déterminé six espaces de réalisation des propriétés du feu :

- 3 espaces de couleurs associés à une propriété éteint, allumé, et même clignotant pour le jaune,
- Le feu éteint toutes ses couleurs sont éteintes,
- Le feu cyclique : en établissant une relation d'exclusion entre la couleur allumée et les couleurs éteintes déterminant trois instances d'un même espace de réalisation et une relation entre ces trois espaces (ici une relation d'ordre),
- Le feu au clignotant : avec la seule réalisation de l'association de jaune et clignotant.

Ces espaces de réalisation représentent l'image de l'espace feu routier à travers le modèle. Nous constaterons par la suite que l'ensemble des autres expressions rationnelles représente le noyau de l'espace feu routier à travers le modèle et que c'est la recherche des relations associant les propriétés élémentaires qui détermine l'espace image.

L'opérateur d'itération "*"

L'opérateur d'itération est un opérateur de relation particulier. Du point de vue des espaces de propriétés, la chronologie n'est pas une variable continue mais doit être compris comme la perception de l'instanciation de cet espace ; la chronologie introduit donc une relation dans la perception que l'on a d'un espace de propriétés.

Considérons E un espace de propriétés quelconque, l'instanciation de cet espace E peut se décrire par la relation entre la réalisation à un instant donné et la réalisation à l'instant suivant, c'est à dire :

$E^0 = \varnothing$, $E^1 = E$, $E^2 = E.E^1$, $E^n = E.E^{n-1}$, $E^{\infty} = \bigvee_{i>0}^{i=\infty} E^i$

Or, l'ensemble des instanciations de l'espace E se définit par E^*.

L'opérateur d'itération introduit précédemment permet de décrire une relation décrivant l'évolution chronologique d'un espace quelconque de propriétés de l'espace général Ω. L'opérateur d'itération "*" ne représente pas le temps ; pas au sens continu mais au sens de l'évolution des espaces à travers les instanciations de leurs propriétés et de leurs relations. Comme pour l'opérateur de relation, cet opérateur ne préjuge pas de la nature de l'évolution. Par exemple, en posant E, l'espace de réalisation du feu routier décrit précédemment, alors, l'expression décrivant la séquence d'évolution est :

- E^1 feu vert équivalente à E^1 = ((vert.allumé).(jaune.éteint).(rouge.éteint)),
- E^2 feu orange équivalente à E^2 = ((vert.éteint).(jaune.allumé).(rouge.éteint)),
- E^3 feu rouge équivalente à E^3 = ((vert.éteint).(jaune.éteint).(rouge.allumé)).
- E^4 feu vert équivalente E^4 = ((vert.allumé).(jaune.éteint).(rouge.éteint)),

En fait, par l'écriture de ces quatre assertions nous avons surtout montré l'existence d'une relation entre trois instances consécutives de l'espace E et l'existence d'expressions rationnelles décrivant l'évolution des trois propriétés.

Le concept d'élément neutre e[∅,e] :

Il y a une propriété du feu que nous n'avons pas abordée : le positionnement des lanternes. Cette propriété peut s'exprimer sous forme des trois propriétés élémentaire : supérieure [{supérieure}, "supérieure"], intermédiaire [{intermédiaire}, "intermédiaire"], inférieure[{inférieure}, "inférieure"]. Cependant, cette propriété n'amène rien dans la description du fonctionnement du feu routier, elle en est une caractéristique descriptive, qui sur notre espace devient une propriété neutre. Lorsque nous parlons du feu routier nous n'utilisons pas des expressions telles que "le feu est rouge fixe" ou le feu est "couleur éteint", mais plutôt "un feu au rouge" ou un "feu éteint". Nous constatons donc que les propriétés significatives pour la description du feu sont :

- éteint[{éteint},"éteint"],
- vert[{vert}, "vert"], jaune[{jaune},"orange"], rouge[{rouge}," rouge"],
- clignotant[{clignotant},"allumé clignotant"].

En effectuant cette opération, nous avons en fait déterminé l'information minimale et pertinente vis-à-vis du comportement du feu. Cependant il est alors possible d'écarter une information qui si elle n'est pas pertinente sur le moment, le devienne par la suite. En effectuant cette recherche de l'information pertinente nous avons appliqué un endomorphisme de monoïde. En d'autre terme, si nous considérons un espace quelconque issu de la description d'une observation, alors la première étape déterminant le modèle est un endomorphisme de monoïde qui va déterminer une image et un noyau.L'image de cet endomorphisme est l'espace des expressions rationnelles décrivant le comportement de l'objet observé. Le noyau de cet endomorphisme est constitué des propriétés observées qui sont neutres vis-à-vis du comportement décrit.

Si E^* décrit l'ensemble des expressions rationnelles d'un espace E, en posant Im(E), l'image de E à travers le modèle et Ker(E) le noyau de E à travers le modèle, étant donné que les expressions du noyau sont neutres vis-à-vis du comportement du modèle alors nous avons $Im(E)^* + Ker(E)^* = Im(E)^*$, avec $Img(E)^* \in E^*$.

En d'autres termes, en décrivant un comportement sous forme d'un nombre fini d'expressions rationnelles on détermine une image (les propriétés significatives identifiées) et un noyau (les propriétés neutres car non significatives) ; chaque introduction d'une nouvelle propriété ou d'une nouvelle relation remet ces caractéristiques en question.

C'est-à-dire que nous vérifions les postulats suivants :

- L'instanciation se définit comme une itération de Img(E),
- L'instanciation de l'espace modélisé observé est déterminée,
- La transformation de cet espace, modifiant Im(E), modifie le comportement.

En particulier, une propriété identifiée mais considérée comme neutre peut changer de statut et transformer le modèle, sans impliquer une reprise du modèle.L'objectif de la démarche est d'admettre une simplification des expressions représentées sans que celle-ci n'induise de biais ni de perte d'information dans la représentation et l'utilisation du modèle de représentation.

Nous avons décrit la séquence vert, jaune, rouge d'un feu routier comme l'expression rationnelle suivante sur E l'espace du feu:

((vert.éteint).(jaune.éteint).(rouge.allumé)) +
((vert.allumé).(jaune.éteint).(rouge.éteint)) +
((vert.éteint).(jaune.allumé).(rouge.éteint)) +
((vert.éteint).(jaune.éteint).(rouge.allumé))

E étant l'espace des propriétés du feu routier en posant :

- vert.eteint $\in$ Ker(E)
- jaune.eteint $\in$ Ker(E)
- rouge.eteint $\in$ Ker(E)
  ou
- couleur.eteint $\in$ Ker(E)

L'expression rationnelle image devient :

rouge.allumé + vert.allumé + jaune.allumé + rouge.allumé

Conclusion de la première étape de conceptualisation

Cette première étape de construction du modèle conceptuel nous a permis d'établir un certain nombre de points dans l'utilisation de l'information. A travers cette représentation sémantique de la propriété nous ne modélisons que l'information utile, celle qui s'échange; par exemple nous n'avons pas ressenti le besoin de préciser la position des trois lanternes, si celle-ci devient pertinente elle viendra compléter la description de l'objet. Si nous posons par convention que l'unité sémantique associée à un domaine de définition est un élément unique qui définit une propriété, l'existence de propriétés dont les domaines de définition sont des singletons qui forment l'unité de base du modèle. Pour une expression rationnelle nous parlons de lettre et de mots, ici les termes de mots et de phrases sont plus appropriés, le sens d'une phrase étant établi à partir des relations entre les mots. Ce sont ces propriétés-mots qui établissent le couplage entre la représentation et le concept.

Même si nous avons défini une notation simplifiée, il faudrait en toute rigueur reprendre la notation complète des propriétés élémentaires car rien ne garantit l'identité entre l'unité sémantique et le concept énoncé. En effet ce qui se symbolise "vert" en France sera "green" en Angleterre sans pour autant changer le nom de la variable portant la donnée de couleur. Néanmoins cette notation complète alourdirait considérablement le modèle de représentation d'un comportement, aussi par convention, les expressions de propriétés élémentaires n'utilisent que l'identifiant. De même, pour des propriétés singleton et quand il n'y a pas d'ambiguïté entre le sens (unité sémantique) et le concept représenté (par exemple la couleur rouge), il est possible de n'utiliser que cette forme allégée de notation.

Tout espace résultant d'une observation sera l'union de l'image et du noyau du morphisme qu'est la modélisation. Par conséquent, en dehors du simple formalisme de conceptualisation et de représentation du modèle, cette notion d'élément neutre trouve aussi son intérêt dans le fait que la description d'un objet quelconque débute par une observation analytique des différentes propriétés qui ne seront pas toutes utiles au modèle. Néanmoins, ces propriétés neutres au début de l'analyse peuvent se révéler utiles à l'introduction de nouvelles relations ou suite de nouvelles observations ; le modèle ne manipule que l'information utile, sans être alourdi par l'information neutre et sans la perdre.

L'établissement du modèle est une opération formelle qui consiste à rechercher les espaces de réalisation établis à partir des relations entre les propriétés. La modélisation peut donc être le résultat d'observation (identification de propriétés et de relations constatées) associé à une opération automatisée.

PROPOSITION D'UNE FORME DES EXPRESSIONS DE COMPORTEMENT

Introduction

Cette première étape dans l'établissement du modèle a permis :

- De décrire un espace particulier comme l'union de propriétés dont certaines sont en relation,
- D'en déduire une représentation exhaustive,
- De décrire la transformation d'un espace à partir de nouvelles propriétés ou de nouvelles relations,

Par contre, nous constatons aussi que l'opérateur "." est pauvre dans la caractérisation de la relation comme dans la description de l'ordre ou de l'instanciation. Rappelons que l'objectif de ces expressions est de décrire un système observable de façon à pouvoir associer un comportement à des propriétés.

S'il n'est pas nécessaire de caractériser la nature des relations, il est indispensable de pouvoir caractériser l'évolution d'un système, c'est-à-dire de représenter une relation d'ordre entre différentes instanciations d'une propriété et par extension d'un espace.

Nous allons donc proposer une représentation algébrique des expressions de comportement décrivant les comportements d'un espace de propriétés :

$$A(X) = \sum_{i=0}^{i=t} p_i \cdot X^i \text{ avec t le nombre de réalisation de la propriété p[P,} \mathscr{I}\text{]}$$

Dans un premier nous allons expliquer la simplification conduisant à cette représentation algébrique et ensuite montrer que l'existence d'un homomorphisme de (Ω, +, . , *, $\in$) dans (Ω, +, .) avec "+" addition et "." produit d'expressions.

Il faut noter que i est la variable d'instanciation; elle définit l'ordre de l'évolution de la propriété p[P, $\mathscr{I}$] sur l'expression A(X). Le produit $p_i.X^i$ représente une relation entre les instances de p et X.

Nous aborderons au chapitre suivant, les apports de cette notation dans la représentation et la manipulation des expressions du comportement des propriétés.

De l'expression rationnelle vers une forme algébrique

Il est nécessaire d'établir une identité entre les éléments manipulés, une approche intuitive nous aidera à bien comprendre l'intérêt de la démarche.

Nous avons déterminé qu'il est possible d'écrire sous la forme d'une expression rationnelle de Ω^* l'évolution ou comportement d'un espace de propriété relativement à l'une de ses propriétés.

En posant X un espace de propriétés quelconque de Ω, alors on notera :

$$A(X) = \sum_{i=0}^{i=t} p_i \cdot X^i$$

L'évolution de l'espace X relativement au comportement A de la propriété p[P, $\mathscr{I}$].

La forme algébrique proposée donne à partir de l'expression de chacun de ses termes les informations suivantes sur le comportement d'un objet quelconque par rapport à une propriété p[P, $\mathcal{I}$] :

- L'opérateur somme indique que l'expression représente une union de réalisations d'une propriété,
- le produit $p_i.X^i$ est défini par l'association de l'instance p_i avec X^i,
- X^i représente l'i-ème itération des parties de X, (pour rappel $X^0 = e[\varnothing,e]$, $X^1=X$, $X^i=X.X^{i-1}$)

Il est donc possible de décrire le comportement d'un objet sous forme d'expressions algébriques d'instances, chaque instance étant elle-même une expression rationnelle élémentaire de propriétés. C'est à dire qu'en écrivant les expressions de comportement chaque coefficient se réfère à une réalisation particulière d'une propriété. Par exemple, prenons pour changer un peu un feu tramway (R17 pour les intimes). La différence avec le feu routier est que les lanternes sont différenciées par leur forme et non par leur couleur.

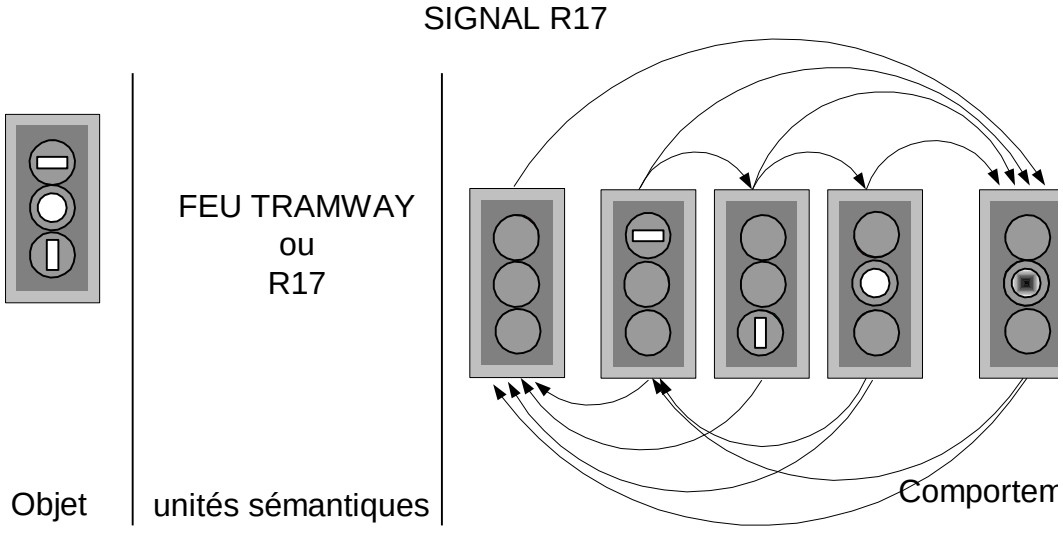


Figure 30 : Feu tramway R17

Pour la compréhension de ce qui suit, nous allons considérer dans un premier une description simplifiée du feu avec les propriétés suivantes:

- disque[{disque}, "disque"],
- vertical[{vertical}, "barre verticale"],
- horizontal[{horizontal}, "barre horizontale"] .

Il est possible à partir de ces trois propriétés de définir un feu routier de tramway

$$C_{R17}(X) = \text{horizontal}.X^i + \text{vertical}.X^{i+1} + \text{disque}.X^{i+2}$$

Nous venons intuitivement de constater qu'il est intéressant de pouvoir manipuler les objets et les propriétés par les expressions algébriques pour la simplification qu'elles apportent dans la description des expressions de comportement.

X est l'espace du feu R17, si nous voulions décrire deux feux il faudrait alors différencier deux espaces X et Y. La description du comportement des deux feux conjointement décrirait alors un espace X.Y résultat d'une relation.

Imaginons un feu R17 et un feu routier protégeant un croisement, dont les expressions de comportement en cycle sont les suivantes :

$$C_{R17}(X) = \text{horizontal}.X^{i} + \text{vertical}.X^{i+1} + \text{disque}.X^{i+2}$$

$$C_{R11}(Y) = \text{vert}.Y^{j} + \text{jaune}.Y^{j+1} + \text{rouge}.Y^{i+2}$$

L'expression rationnelle d'une séquence de feu pourrait alors s'écrire ainsi:

$C(Z) = (\text{horizontal}.X^{i}).(\text{vert}.Y^{j}) + (\text{horizontal}.X^{i}).(\text{jaune}.Y^{j+1}) + (\text{horizontal}.X^{i}).(\text{rouge}.Y^{i+2}) + (\text{rouge}.Y^{i+2}).(\text{vertical}.X^{i+1}) + (\text{rouge}.Y^{i+2}).(\text{disque}.X^{i+2}).\ (\text{rouge}.Y^{i+2}).(\ \text{horizontal}.X^{i+3})$

Nous voyons qu'il devient intéressant de pouvoir définir l'espace X comme une variable espace quelconque représentant l'espace dont l'évolution est le résultat d'une relation avec les propriétés décrites, ce de façon à pouvoir établir une expression du type :

$C(X) = \text{horizontal}.\ (\text{vert}X^{k} + \text{jaune}X^{k+1} + \text{rouge}X^{k+2}) + \text{rouge}.(\text{vertical}.X^{k+3} + \text{disque}X^{k+4} + \text{horizontal}.X^{k+5})$

avec k=i+j,

qui montre clairement la relation existant entre la séquence d'un feu et l'état "fermé" de l'autre feu.

Pour cela il est nécessaire d'aller au-delà du simple couplage intuitif et d'établir un homomorphisme entre les expressions rationnelles (Ω, +, ., *, $\in$) et les formes algébriques sur (Ω, +, .).

Définition d'un espace algébrique des expressions

Nous allons donc définir une application de (Ω, +, . , *, $\in$) dans (Ω, +, .) dont nous vérifierons les propriétés d'homomorphisme.

Soit une propriété quelconque p[P, $\mathcal{I}$], nous allons donc définir l'application suivante qui à une expression rationnelle du comportement de cette propriété fait correspondre une expression algébrique :

de $(\Omega, +, ., *, \in) \rightarrow (\Omega, +, .)$

$$A = \sum_{i=0}^{i=t} p_i \qquad \alpha \qquad A(X) = \sum_{i=0}^{i=t} p_i \cdot X^{i}$$

et nous vérifierons les propriétés de l'homomorphisme.

L'application ainsi définie fait correspondre à une propriété quelconque isolée, un espace sur lequel elle s'instancie.

Le caractère homomorphique de cette application sera vérifié si quelque soient p[P, $\mathcal{I}$] et q[Q, $\mathcal{A}$] propriétés sur Ω :

- $P+Q \leftrightarrow P(X)+Q(X)$
- $P.Q \leftrightarrow P(X).Q(X)$

Ces deux propositions s'admettent facilement à partir de la définition du domaine de définition P d'une propriété comme ensemble des réalisations de cette propriété. L'expression rationnelle du domaine fournissant la somme des instances, l'expression de comportement enrichissant cet ensemble d'une relation d'ordre.

A titre d'exemple d'illustration, prenons simplement deux lampes respectivement verte et rouge dont les espaces de réalisations peuvent se décrire :

vert = {vert.éteint.P^i, vert.clignotant.P^{i+1}, vert.fixe.P^{i+2}}

et

rouge = {rouge.éteint.Q^j + rouge.allumé.Q^{j+1}}

avec i et j quelconques ≥ 0.

Ces 2 expressions rationnelles signifient

- que pour la lampe verte les états *éteint*, *clignotant* et *fixe* sont liés par une relation d'ordre (séquence).
- Que pour la lampe rouge, les 2 propriétés sont aussi reliées par une relation d'ordre.

Remarque : la précision sur les relations d'ordre entre les deux propriétés indépendantes (eteint et allumé) peut paraître inutile car naturelle; simplement n'oublions pas que cet exemple doit rester représentatif du cas général pour lequel les propriétés ne sont pas forcément indépendantes.

Définissons les expressions du comportement des propriétés de ces objets.

vert(X) = vert.éteint.X^i + vert.clignotant.X^{i+2} + vert.fixe.X^{i+3}

rouge(Y) = rouge.éteint.Y^j + rouge.allumé.Y^{j+2}

La proposition P+Q $\leftrightarrow$ P(X)+Q(Y) s'admet immédiatement car chaque objet décrit un espace indépendant.

P+Q = {vert.éteint.P^1, vert.fixe.P^2, vert.clignotant.P^3 }$\cup${ rouge.éteint.Q^1, rouge.allumé.Q^2}

et

vert(X) + rouge(Y) = vert.éteint.X^1 + vert.clignotant.X^2 + vert.fixe.X^3 + rouge.eteint.Y^1 + rouge.alluméY^2

Ce qui signifie que si les espaces des lampes verte et rouge s'instancient indépendamment l'union de ces deux espaces de propriétés est équivalente à la somme des expressions du comportement des propriétés.

Pour montrer la proposition P.Q $\leftrightarrow$ P(X).Q(Y) rappelons que d'après la définition de l'opération "." la relation des deux espaces de réalisation produit un espace

PxQ = {p.q | p $\in$ { vert.éteint.P^1, vert.fixe.P^2, vert.clignotant.P^3}, q $\in$ { rouge.éteint.Q^1, rouge.allumé.Q^2 }}

L'expression rationnelle résultant de la relation sera :

(vert.eteint).(rouge.eteint) + (vert.eteint).(rouge.allumé) + (vert.fixe).(rouge.eteint) + (vert.fixe).(rouge.allumé) + (vert.clignotant).(rouge.eteint) + (vert.cligontant).(rouge.allumé)

Nous pouvons facilement déterminer l'expression de comportement définit par le produit :

vert(X).rouge(Y) = (vert.eteint.X).(rouge.eteint.Y) + (vert.eteint.X).(rouge.allumé.Y^2) + (vert.clignotant.X^2).(rouge.eteint.Y) + (vert.clignotant.X^2).(rouge.alluméY^2) + (vert.fixe.X^3).(rouge.eteint.Y) + (vert.fixe.X^3).(rouge.allumé.Y)

Or poser qu'il existe une relation entre l'espace de la lampe verte et l'espace de la lampe rouge implique que les expressions de comportement s'expriment sur un même espace Z.

D'où l'expression du produit :

vert(Z).rouge(Z) = (vert.éteint).(rouge.eteint).Z^2 + (vert.éteint).(rouge.allumé).Z^3 + (vert.clignotant).(rouge.eteint).Z^3 + (vert.clignotant).(rouge.allumé).Z^4 + (vert.fixe).(rouge.eteint).Z^4 + (vert.fixe).(rouge.allumé).Z^5

On retrouve dans le produit l'expression des 6 combinaisons d'états p.q des propriétés de PxQ.

Nous venons de montrer l'existence d'un homomorphisme

de $(\Omega, +, ., *, \in) \rightarrow (\Omega, +, .)$

$$P = \sum_{i=0}^{i=t} p_i \quad \alpha \quad P(X) = \sum_{i=0}^{i=t} p_i X^i$$

Où i est l'ordre de l'instanciation de la propriété p et de l'espace X par conséquent.

Définition des opérateurs d'expressions de comportement

L'objectif de décrire un comportement sous cette forme réside essentiellement dans le fait qu'elle permet de formuler des comportements de propriétés sous forme d'expressions pour lesquelles X représente un espace indifférencié associé à la propriété et ainsi de pouvoir manipuler ces expressions avec les opérateurs somme et produit. Définissons les deux opérations somme et produit d'expressions correspondant à la construction d'espaces de réalisation de propriétés indépendantes et de propriétés dépendantes (ou en relation) comme suit :

Somme de deux expressions :

En notant $A(X) = \sum_{n\geq 0} p_n X^n$ et $B(X) = \sum_{n\geq 0} q_n X^n$ alors $A(X) + B(X) = \sum_{n\geq 0} (p_n + q_n) \cdot X^n$

L'élément neutre de l'addition est l'expression du comportement de la propriété $\in[\varnothing,\in]$,

$$\in X^0 = \in$$

Nota : l'élément neutre ne se définit pas comme une absence de comportement. En effet, dans ce cas l'absence de comportement impliquerait la propriété n'évolue pas; par exemple pour p, que $A(X) = p_0$ quelque soit n>0. Or cette expression ne peut être considérée comme neutre pour l'addition car dans ce cas la propriété continue d'être associée au comportement décrit par l'expression rationnelle. Or, l'expression $\in X^0$ définit un comportement sans existence vis-à-vis du projet d'action, c'est-à-dire le comportement de propriétés neutres vis-à-vis du projet d'action.

Produit de deux expressions :

En notant $A(X) = \sum_{n\geq 0} p_n \cdot X^n$ et $B(X) = \sum_{m\geq 0} q_m \cdot X^m$ alors on définit

$$A(X).B(X) = \sum_{i=0}^{i=n+m} \sum_{n+m=i} p_n \cdot q_m \cdot X^i ,$$

le produit des deux expressions.

Avant de déterminer l'élément neutre de cet opérateur, le choix de ce produit nécessite quelques explications. Sachant que i est la variable d'instanciation; elle définit l'ordre de l'évolution de l'espace de propriété X; c'est-à-dire que la i-ème instance de X^i ne peut être que le résultat de i instances p_n et q_m de p[P, $\mathcal{I}$] et q[Q, $\mathcal{A}$], tel que n+m=i.

En remarquant que l'élément neutre de la somme, $\in X^0$, est aussi l'élément neutre du produit de deux expressions, nous pouvons admettre l'existence de l'anneau (Ω, + , .).

Conclusion de la seconde étape de conceptualisation

Il faut noter que le couplage que nous venons d'établir en montrant l'existence d'un homomorphisme d'un espace d'expressions rationnelles vers un espace algébrique est l'élément fondamental de l'utilité et de l'utilisabilité de cette approche. Dans la représentation de la dynamique de l'instanciation, l'objet est porteur de ce qui caractérise ses changements d'état mais pas de ce qui les provoque. Ainsi, à travers ces expressions il est vraiment possible de caractériser les évolutions d'un espace quelconque de propriétés à travers sa relation avec les réalisations de ses propriétés. Le choix du système d'écriture formel d'une propriété associant sémantique et valeurs des réalisations permet une transposition directe de l'expression rationnelle sémantique vers l'expression de comportement. En effet, dans la définition donnée d'une propriété p[P, $\mathcal{I}$], chaque entité identifiée représente un élément d'un langage composant l'espace général Ω, à partir duquel nous établissons des expressions. On remarquera que chaque propriété élémentaire peut être associée à une lettre. Ainsi, dans le modèle, chaque entité du modèle est générée et peut être générée à partir de propriétés élémentaires du modèle. Cependant, cette règle étant établie, chaque entité est parfaitement déterminée et le modèle ne permet alors plus de prendre en compte les problèmes liés aux échanges humains; c'est la raison pour laquelle, la définition complète d'une propriété intègre son domaine de définition et son unité sémantique.

Enfin, nous avons montré à partir de la définition d'un élément neutre que la modélisation proposée est en fait l'image d'un morphisme de l'espace observable vers un espace observé, mais que l'information non utilisée n'est en aucun cas "oubliée". C'est-à-dire que la modélisation d'un espace de propriété sera constituée de la description de la propriété, dont son domaine de définition, et des expressions de ses comportements.

Nous allons donc dans la suite de ce mémoire aborder deux sujets :

- l'intérêt de la représentation sous forme d'expressions d'une propriété et de son comportement et les outils de manipulation qu'il est possible d'y associer
- mais aussi la quasi isomorphie entre le modèle de représentation et la chose décrite.

UTILISATION DES EXPRESSIONS DE COMPORTEMENT DANS LA MODELISATION

Expression d'un comportement répétitif

Si nous examinons les expressions descriptives du feu tramway R17 nous pouvons constater que celles-ci respectent l'ordre des différents états mais ne représentent pas le comportement répétitif ou l'aspect cyclique du comportement de chacune des propriétés. Prenons

une première expression qui représente la succession des états en fonctionnement ou éteint du feu : forme(X) = horizontal.X+ vertical.X^2+ disque.X^3.
L'expression écrite indique seulement qu'après l'état horizontal vient l'état vertical puis l'état disque; nous avons défini un ordre dans l'instanciation de la propriété. Pour être complète l'expression devrait être :
Horizontal.X + vertical.X^2+ disque.X^3+ ⋯ + horizontal.X^n + vertical.X^{n+1}+ disque.X^{n+2}+ ⋯

Il apparaît de façon évidente dans cette expression une structure répétitive - un motif – "horizontal.X^n + vertical.X^{n+1}+ disque.X^{n+2}" répétée à l'infini.

En posant comme expression de la forme du signal, l'expression suivante :

$$\text{forme}(X) = \sum_{n=0}^{n=+\infty} (\text{horizontal}.X^n + \text{vertical}.X^{n+1} + \text{allumé}.X^{n+2})$$

équivalente à :

$$\text{forme}(X) = \sum_{n=0}^{n=+\infty} (\text{horizontal}.X^0 + \text{vertical}.X^1 + \text{allumé}.X^2).X^n$$

nous représentons l'aspect cyclique du comportement.

Pour des expressions décrivant des comportements cycliques ou répétitifs on admettra une notation simplifiée :

forme(X) = (horizontal.X^n + vertical.X^{n+1}+ disque.X^{n+2})

ou

forme(X) = (horizontal.X^0 + vertical.X^1+ disque.X^2).X^n

Dans le cas présent l'indice *n* est défini de 0 à +∞ mais cet indice peut être défini sur un intervalle fini quelconque.

Une expression peut décrire un état initial, un motif et un état final, par exemple, l'expression suivante :

$$\text{Comportement}(X) = \text{eteint}.X^0 + \sum_{n=1}^{n=10} (\text{jaune}.X^n + \text{rouge}.X^{n+1} + \text{vert}.X^{n+2}) + \text{éteint}.X^{11},$$

décrit un enchaînement d'un état éteint, suivi de dix cycles jaune, rouge, vert, se terminant par un retour à l'état éteint.

1.1.1 Expression d'une chronologie

On remarque aisément que l'expression d'un comportement itératif traduit la chronologie d'une séquence. Cependant, l'introduction d'une chronologie implique forcément un ordre entre les instances et par conséquent l'existence une instance de départ. Considérons deux signaux protégeant des voies voie routière et voie tramway :

$$R17(X) = \sum_{n=0}^{n=+\infty} (\text{horizontal}.X^n + \text{vertical}.X^{n+1} + \text{disque}.X^{n+2})$$

$$R11(X) = \sum_{m=0}^{m=+\infty} (\text{rouge}.X^m + \text{vert}.X^{m+1} + \text{jaune}.X^{m+2})$$

La chronologie établie sur chacune de ces 2 expressions traduit l'ordre de séquences pour lesquelles nous avons arbitrairement choisi les instances *horizontal* et *rouge* comme instances de départ. En établissant la relation m = n + 1, il est possible de synchroniser ces séquences pour gérer deux voies antagonistes. L'expression du feu routier devient :

$$R11(X) = \sum_{n=0}^{n=+\infty} (rouge.X^{n+1} + vert.X^{n+2} + jaune.X^{n+3})$$

On obtient le produit :

$$R17(X).R11(X) = \sum_{n=0}^{n=+\infty} (horizontal.rouge.X^{2n+1} + (horizontal.vert + vertical.rouge).X^{2n+2} + (vertical.vert + horizontal.jaune + disque.rouge).X^{2n+3} + (vertical.jaune + disque.vert).X^{2n+4} + disque.jaune.X^{4}).X^{2n+5}$$

Expressions de comportement, graphes, matrices et automates

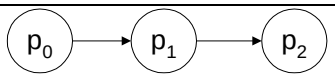
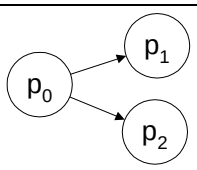
Nous pouvons remarquer à travers ces différentes formes que l'expression décrit un système composé d'un ensemble d'états et des différentes transitions entre ces états. C'est-à-dire un système de transitions.

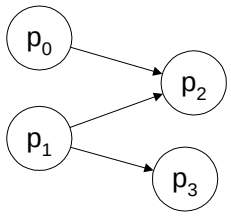
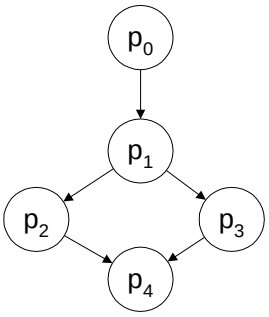
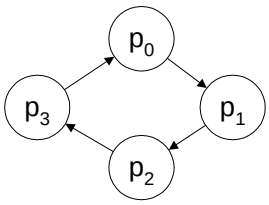
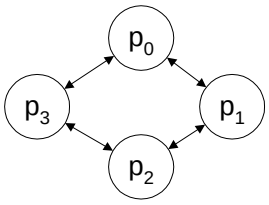
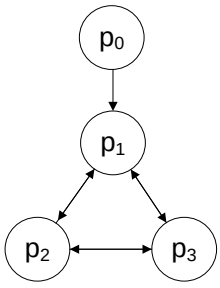
Ainsi, le comportement d'un système vis-à-vis d'un état donné peut être décrit par le graphe des transitions conduisant vers cet état et par extension il est possible de décrire l'ensemble des actions possibles comme le graphe des transitions partant de cet état.

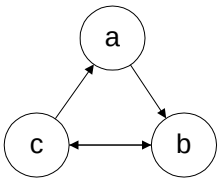
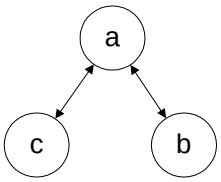
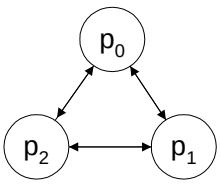
Soit la propriété p [P, $\mathscr{I}$] , p_i et p_j des instances quelconques de p [P, $\mathscr{I}$] on note $\delta_{i,j}$ la fonction d'instanciation de p [P, $\mathscr{I}$] avec $\delta_{i,j} = 1$ s'il existe une transition de la réalisation p_i vers la réalisation p_j, $\delta_{i,j} = 0$ sinon.

La fonction d'instanciation peut être décrite comme une matrice avec en ligne les instances des états de départ et en colonne les instances des états d'arrivée. On appellera cette matrice la matrice d'instanciation de la propriété. La matrice d'instanciation définit un graphe dont les nœuds sont les instances et les arêtes les transitions possibles.

Le tableau ci-dessous résume différentes structures de graphes, d'expressions de comportement et matricielles associées :

Graphe	représentation graphique	expression de comportement	matrice d'instanciation
Chaîne		$p_0.X^0 + p_1.X^1 + p_2.X^2$	$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$
Arbre		$p_0.X^0 + (p_1+p_2).X^1$	$\begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$

Graphe	représentation graphique	expression de comportement	matrice d'instanciation
Poly-arbre		Le comportemetn se décrit par 2 expressions : $p_0.X^0 + p_2.X^1$ et $p_1.X^0 + (p_2+p_3)X^1$	$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$
graphe avec choix		$p_0.X^0 + p_1.X^1 + (p_2+p_3).X^2 + p_4.X^3$	$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$
graphe cyclique orienté avec p_0 état initial		$p_0.X^n + p_1.X^{n+1} + p_2.X^{n+2} + p_3.X^{n+3}$	$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$
graphe cyclique non orienté		$(p_0+ p_2).X^n + (p_1+ p_3).X^{n+1}$	$\begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}$
Avec état d'entrée fixé		$p_0.X^0 + p_1.X^1 + (p_{2+} p_3).X^2 + (p_1+p_2+p_3).X^n$	$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$

Graphe	représentation graphique	expression de comportement	matrice d'instanciation
cycle a – b –c et d'un cycle b -c		$(a+b).X^n + (b+c).X^{n+1}$	$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$
2 cycles reliés par un noeud		$a.X^n + (b+ c).X^{n+1}$	$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}$
Espace sans condition de transition		$(p_0+p_1+p_2).X^n$	$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$

Avant d'aborder l'intérêt que présente le fait de pouvoir manipuler ces différentes formes de représentation, il faut noter que chacune possède une richesse intrinsèque dans la description du comportement et l'utilisation.

La forme graphe :

Le graphe est une des premières formes naturelles que nous utilisons pour appréhender un système à changement d'états ou un système à transitions. Cependant, l'exploitation du graphe implique forcément de fixer un départ et un certains nombre d'instanciations pour déterminer un chemin. Lorsqu'on veut réaliser une approche globale d'analyse et d'évaluation cette approche ne peut pas être considérée comme systématique.

La forme matricielle :

La matrice de transition est la forme de représentation d'un espace de réalisation donné qui offre des facilités de manipulation.

L'expression de comportement proposée:

Si le graphe et la matrice décrivent la structure d'un espace de réalisation, la forme d'expression proposée décrit les changements d'état de l'espace de réalisation, mais décrit aussi la structure de l'espace de réalisation. Par exemple, le poly-arbre qui implique que l'espace de

réalisation est partitionné en deux sous espaces sur lesquels la propriété p[P, $\mathcal{A}$] s'instancie alternativement. La forme d'expression proposée semble offrir à la fois une description générale de l'espace de réalisation et une description systématique des différents états de cet espace, certaines lourdeurs de notations (grandes expressions) ou une représentation plus schématique des états transitions, justifient le fait de pouvoir manipuler les trois formes de représentation.

Nous allons donc étudier succinctement le passage d'une forme à l'autre.

Vers la forme graphe :

Que ce soit depuis la forme expression de comportement ou la forme matricielle, le passage au graphe consiste à passer d'une représentation littérale à une représentation graphique.

Depuis la forme matricielle, cette conversion se fait naturellement. On remarquera simplement au passage:

- que chaque colonne dont la somme des termes est nulle, correspond à une instance qui ne peut être atteinte qu'à l'état initial,
- que chaque ligne dont la somme est zéro correspond à une instance seulement terminale,
- que chaque matrice (ou sous matrice) dont la somme des termes en ligne et en colonne est 1, correspond à un graphe (ou sous graphe) cyclique,
- que la symétrie par rapport à la diagonale traduit le fait que les transitions ne sont pas orientées.

Depuis l'expression de comportement, la conversion est effectuée par une lecture interprétation. Chaque nouvelle valeur de propriété rencontrée ajoute un nouveau nœud, chaque transition aX^n vers bX^{n+1} implique l'existence d'une transition orientée de a vers b.

Du graphe à l'expression de comportement :

Ainsi que nous l'avons abordé dans le paragraphe précédent, il est possible de déterminer une expression de comportement en traduisant le parcours sur le graphe jusqu'à mettre en évidence les motifs. Il est possible aussi de chercher dans un graphe des motifs connus pour en déduire des expressions.

Le passage à la forme matricielle :

Depuis l'expression de comportement, la conversion est effectuée par une lecture interprétation. Chaque transition aX^n vers bX^{n+1} que la valeur correspondant à la ligne de *a* et à la colonne de *b* de la matrice a pour valeur 1 .

Nous avons montré que la formalisation du concept de propriété permet de définir toute propriété à partir d'expressions de comportement sur l'espace général. La représentation matricielle est intéressante par le fait qu'elle assure le lien avec les systèmes de transitions étiquetées : un automate, dont les transitions respecteront la représentation établie.

EXPRESSIONS DE COMPORTEMENT, OPERATEURS ET RELATIONS

Nous avons décrit la relation au sens large sous la forme d'un opérateur. L'expression de la relation se fait naturellement car elle correspond à la perception la plus évidente que nous ayons d'une structure ou d'une organisation. La notion qui vient immédiatement à l'esprit pour ce type d'ensemble est celle de l'objet, mais celle-ci étant trop réduite aux limites physiques qui sont sous entendus, nous avons naturellement élargi le concept à l'espace de propriétés. L'espace de propriétés étant en fait la perception que nous avons d'un objet, de ses propriétés et de leurs comportements.

Nous avons établi précédemment que les relations qui caractérisent une communauté de propriétés sont de cinq grandes catégories : généricité, association, partage, dépendance, influence. Nous avons aussi établi un modèle de représentation à partir d'une définition de la propriété et d'opérateurs. Si intuitivement on pressent que les formes choisies permettent de décrire propriétés et comportements, il est nécessaire de compléter l'approche modélisatrice en expliquant comment différencier la nature des relations entre propriétés et comment les représenter. Pour cela, nous allons revenir à notre exemple de feu tramway et à partir d'une démarche d'analyse descriptive expliquer la représentation des relations par les expressions de comportement.

L'opérateur "+" représente l'union de différentes instances. Si nous "additionnons" les instances d'un même espace, nous obtenons une information sur cet espace, si nous additionnons des instances d'espaces différents, nous n'avons rien de plus qu'une concomitance de deux états indépendants.

A contrario, l'opérateur "." indique la mise en relation de propriétés c'est-à-dire que la relation entre p[P, $\mathscr{P}$] et q[Q, $\mathscr{Q}$] définit un nouvel espace de propriétés. Nous allons donc détailler un peu l'utilisation de ces opérateurs, et les relations sous jacentes dans la définition des expressions de comportement. Nous allons voir dans ce paragraphe que la mise en relation de propriétés ne correspond pas à une nouvelle instanciation de ces propriétés mais à la création d'un nouvel espace. C'est la raison pour laquelle la définition de l'opérateur de relation est :

p[P, $\mathscr{P}$] . q[Q, $\mathscr{Q}$] = (p.q)[P.Q =$\{ p_i.q_i \mid p_i \in P , q_i \in Q \}$, ($\mathscr{P}$en relation avec $\mathscr{Q}$)],

et non, p[P, $\mathscr{P}$] . q[Q, $\mathscr{Q}$] = (p.q)[P × Q, ($\mathscr{P}$en relation avec $\mathscr{Q}$)].

Dans ce cas la définition correcte aurait dû être p.q[P × Q → Z, ($\mathscr{P}$en relation avec $\mathscr{Q}$)] ce qui aurait généré l'apparition dans la notation d'un objet non complètement défini.

Revenons à notre feu tramway pour lequel nous n'avons dans les exemples précédents volontairement considéré que peu de propriétés, et ce, sans condition particulière.

Dans les exemples précédents, nous n'avons pas distingué les trois lanternes et leur position respective. En fait, la démarche avait déjà sous une certaine forme intégrée la perception que nous avons du feu et de son comportement. L'intellect effectue naturellement certaines simplifications et certaines associations. De même pour la compréhension nous avons choisi, dans les paragraphes précédents, d'associer sans condition ni restriction les deux propriétés forme et fonctionnement du feu tramway, or, dans la définition de cet objet il existe des restrictions sur la nature des relations entre les propriétés. Nous observons que le feu est composé de trois signaux lumineux positionnés verticalement, que les formes de ces signaux sont une barre verticale en position inférieure, un disque au centre et une barre horizontale en position supérieure. Notre connaissance du comportement du feu nous indique qu'un seul signal est allumé à la fois, que seul le disque peut être clignotant, et que les signaux se succèdent toujours dans l'ordre barre horizontale, barre verticale, disque, barre horizontale. Enfin, l'allumage du feu ou un défaut quelconque conduisent à une phase clignotante. En résumé le feu en tant qu'objet a trois états : *éteint*, *disque clignotant* ou *fonctionnement cyclique*.

Dans un premier temps nous pouvons identifier toutes les propriétés élémentaires énoncées :

- les propriétés fixe[{fixe}, "allumé fixe"], éteint[{éteint},"éteint"], clignotant[{clignotant},"allumé clignotant"],
- les propriétés disque[{disque}, "disque"] + vertical[{vertical}, "barre verticale"] + horizontal[{horizontal}, "barre horizontale"].

La description du feu tramway va maintenant consister à décrire à partir d'expression de comportement des espaces de propriétés et des espaces de réalisation. Si nous admettons de percevoir le feu comme un tout, nous pouvons décomposer ce qui le compose de différentes

façons : en s'attachant aux objets physiques que nous voyons et en essayant de décrire les relations qui les unissent, ou en s'attachant à la globalité du feu et en décrivant ce que nous percevons. En fait, nous constaterons que ces deux approches aboutissent au même résultat.

Le feu observé se décompose en trois signaux a priori indépendants positionnés verticalement. La barre horizontale interdit le passage, la barre verticale autorise le passage, le disque signale le passage dans un bref délai à la barre horizontale. Si nous décidons de décrire le feu par les objets physiques, nous obtiendrons trois signaux indépendants dont la description comprend les propriétés élémentaires de position et forme et les propriétés décrivant l'état de fonctionnement. Par exemple : signal1(X) = horizontal.(éteintX^k + fixeX^{k+1}). Avant d'aller plus loin dans le raisonnement de la description, faisons une première constatation. Nous avons décrit un objet feu comme l'association de trois propriétés indépendantes. Ces trois propriétés étant elles-mêmes une association de propriétés élémentaires et d'une propriété plus complexe que nous avons exprimée entre parenthèses : (éteintX^k + fixeX^{k+1}).

Nous avons utilisé là la première forme de relation : l'*association*.

La relation d'association est la forme la plus générale de relation. Les relations d'associations décrivent l'abstraction d'un couplage existant entre des propriétés; c'est-à-dire que la réalisation d'une relation d'association existe par la réalisation particulière de deux propriétés indépendantes. Par exemple, le jaune clignotant de notre signal est l'association de la réalisation jaune de la propriété couleur et de la réalisation de la propriété clignotant; néanmoins ces deux propriétés ne sont pas dépendantes. L'association peut aussi prendre une forme plus générale comme par exemple lorsque nous avons défini l'association de l'état allumé fixe du feu avec la propriété globale de couleur du feu.

Une relation d'association décrit une nouvelle unité sémantique munie d'un identifiant et d'un domaine de définition. La définition du premier signal est la suivante : signal1[{horizontal.eteint, horizontal.fixe}, "signal1"]

La relation d'association peut se formaliser ainsi : étant donnés p[P, $\mathcal{P}$], q[Q, $\mathcal{Q}$] et z[Z, $\mathcal{Z}$] objets ou propriétés sur Ω alors la relation d'association de p[P, $\mathcal{P}$] et q[Q, $\mathcal{Q}$] se définit par l'objet ou la propriété z[Z, $\mathcal{Z}$] si et seulement si z => p ∧ q. Si la condition ne porte que sur certaines réalisation de p[P, $\mathcal{P}$] et q[Q, $\mathcal{Q}$] alors c'est une association de réalisation, on la notera par les expressions rationnelles de la forme p.q, si l'association porte sur l'ensemble des réalisations c'est une association d'espaces, on la notera par une expression rationnelle de la forme P ∪ Q.

Continuons avec notre premier signal et remarquons que nous avons directement utilisé l'expression de comportement; mais le signal1 aurait pu être précédemment décrit par une expression horizontal.(eteint + fixe) qui signifie que le signal se reconnaît par les deux instances indépendantes suivantes: horizontal.eteint et horizontal.fixe .

Pour simplifier l'expression nous aurions pu définir une propriété état[{eteint, fixe},"état"] et décrire le signal1 par l'expression horizontal.état et par extension les deux autres signaux par les expressions disque.état et vertical.état .

Nous avons utilisé là la première forme de relation : la *généricité*.

Les relations de généricité impliquent une communauté de propriétés entre deux espaces différents. On parle de généralisation lorsque la relation peut s'exprimer ainsi : étant donnés p[P, $\mathcal{P}$], q[Q, $\mathcal{Q}$] et z[Z, $\mathcal{Z}$] espaces de propriétés sur Ω alors z[Z, $\mathcal{Z}$] est une généralisation de p[P, $\mathcal{P}$] et q[Q, $\mathcal{Q}$] si et seulement si z => p □ q=>z et P⊂ Z, Q ⊂ Z.

C'est-à-dire qu'on pourra utiliser z[Z, $\mathcal{Z}$] en remplacement de p[P, $\mathcal{P}$] et q[Q, $\mathcal{Q}$] dans certaines expressions.

Cette relation est une unité sémantique décrivant une forme de factorisation de propriétés communes à des espaces différents sous forme d'un espace représentatif. La relation de généralisation construit un espace de propriétés qui est la représentation d'une partition commune aux espaces que nous voulons représenter. La relation est alors l'expression de l'existence d'un comportement endomorphe à cette partition. On peut aussi parler de factorisation de propriétés, c'est pourquoi nous avons choisi d'illustrer cette relation par un premier exemple sur l'état du signal. Pour illustrer la généricité avec un exemple plus pertinent, revenons sur le feu routier; imaginons maintenant que nous voulons sécuriser un croisement avec une ligne de tramway. Nous avons donc besoin de fournir au conducteur de la rame le même type d'information sur l'autorisation ou l'interdiction de traverser, et sur l'imminence de la fin d'interdiction de traverser. Cependant, le tramway connaît et respecte aussi une signalisation propre au domaine ferroviaire. Comment alors éviter l'ambiguïté sur l'information d'un vert ou d'un rouge l'un sécurisant une traversée routière, l'autre une circulation tramway? De même, il est nécessaire de pouvoir différencier les signaux pour une voie routière parallèle à une voie tramway. Pour cela les couleurs ont été remplacées par des formes de couleur blanche (barre verticale pour le vert, disque pour le jaune, barre horizontale pour le rouge), c'est le feu R17 que nous utilisons. Il est ainsi possible de définir un objet générique décrivant le fonctionnement d'un feu et de l'utiliser dans la description d'un feu R11 ou d'un R17 en complétant les propriétés des lanternes par les couleurs ou les formes appropriées.

L'autre expression de la généricité qui vient alors naturellement est la *spécialisation* qui peut s'exprimer comme suit : étant donnés p[P, $\mathcal{P}$], q[Q, $\mathcal{Q}$] et z[Z, $\mathcal{Z}$] espaces de propriétés sur Ω alors p[P, $\mathcal{P}$] et q[Q, $\mathcal{Q}$] sont des spécialisations de z[Z, $\mathcal{Z}$] si et seulement si z => p □ q et P⊂ Z, Q ⊂ Z.

Il est évident que la définition de la spécialisation est la même que celle de la généralisation. Elle exprime cependant la relation non pas sous son aspect factorisation mais sous un aspect différentiation. Pour bien comprendre la nuance, abusons de l'exemple du feu routier. Nous avons défini précédemment le feu R11 à trois couleurs (vert, jaune, rouge). Le vert indique un passage autorisé et protégé. Il peut être utile d'autoriser ce passage alors que le feu ne peut entièrement le protéger. Ce type de passage autorisé mais non protégé existe avec la position jaune centrale mise au clignotant. L'automobiliste interprète l'information comme une autorisation de passage mais sans protection. Cependant cet état indique aussi que l'ensemble du carrefour est soumis à cette règle, il n'y alors plus de régulation des flux. Il est parfois nécessaire pour la régulation du trafic d'autoriser une voie de circulation non protégée. Dans ce cas la lanterne verte est transformée en une lanterne jaune clignotant pour donner les deux informations le passage est autorisé mais non protégé. Ceci est possible car l'automobiliste associe la position du signal à l'information lumineuse. Il ya spécialisation du feu R11 en un feu R11j comportant les trois informations (jaune clignotant, jaune, rouge). La séquence de signaux n'est pas modifiée, seule une des propriétés change.

Nous venons à travers la première description d'aborder deux des cinq formes de relations.

L'association des propriétés implique qu'il y a indépendance des comportements de ces propriétés l'une vis-à-vis de l'autre. C'est-à-dire que l'ensemble des évolutions en fonction de chaque réalisation de chacune des propriétés doit couvrir toutes les combinaisons de cas. L'expression de comportement de l'espace de réalisation X en fonction des deux propriétés sera déterminée par les produits des expressions $P(X) = \sum_{n=0}^{n=t} p_n \cdot X^n$ et $Q(X) = \sum_{m=0}^{m=t'} q_m \cdot X^m$,

Soit Z l'espace de comportement construit par l'association de deux objets définissant les espaces de comportement indépendants X et Y, espaces de réalisation des propriétés p[P, $\mathcal{P}$] et q[Q, $\mathcal{Q}$].

Le comportement de chacun des objets étant décrit respectivement par les expressions :

$$\sum_{n=0}^{n=t} p_n \cdot X^n \text{ et } \sum_{m=0}^{m=t'} q_m \cdot X^m ,$$

dans ce cas, l'expression de comportement de l'espace Z=X.Y sera décrit par l'expression :

$$\sum_{i=0}^{i=t+t'} \sum_{n+m=i} p_n \cdot q_m \cdot Z^i = \sum_{n=0}^{n=t} p_n \cdot X^n \cdot \sum_{m=0}^{m=t'} q_m \cdot X^m$$

Cette relation est la plus riche et aussi la plus difficile à manipuler. En effet, une association définit bien une communauté de propriétés, pas forcément une communauté de comportement.

Pour marquer la différence d'instanciation nous noterons différemment l'exposant d'itération et l'indice d'instanciation.

Reprenons et complétons la description des trois signaux du feu tramway:

signal1(X) = horizontal.(éteint + fixe)X^k avec k ∈ [1, ∞]

signal3(X) = vertical.(éteint + fixe)X^n avec n ∈ [1, ∞]

C'est-à-dire que les signaux 1 et 3 sont représentés par une propriété invariante et par un comportement : éteint ou allumé fixe.

signal2(X) = disque.((éteint+clignotant).X^m + (clignotant + fixe).X^{m+1}) avec m ∈ [1, h]

De même, le signal 2 est représenté par une propriété invariante mais un comportement plus complexe : éteint, allumé fixe ou allumé clignotant.

Le feu lui-même est donc l'association des ces trois signaux, ce qui s'écrit :

feu(X) = signal1(X).signal2(X).signal3(X)

= horizontal.(éteint+fixe)X^k.disque.(éteint+clignotant+fixe)X^m.vertical.(éteint+fixe)X^n

= (horizontal.éteint.disque.éteint.vertical.éteint+horizontal.éteint.disque.éteint.vertical.fixe + horizontal.éteint.disque.clignotant.vertical.éteint + orizontal.éteint.disque.clignotant.vertical.fixe + horizontal.éteint.disque.fixe.vertical.éteint + horizontal.éteint.disque.fixe.vertical.fixe + horizontal.fixe.disque.éteint.vertical.éteint + horizontal.fixe.disque.éteint.vertical.fixe + horizontal.fixe.disque.clignotant.vertical.éteint + horizontal.fixe.disque.clignotant.vertical.fixe + horizontal.fixe.disque.fixe.vertical.éteint + horizontal.fixe.disque.fixe.vertical.fixe).X^{k+m+n}

Il faut remarquer que dans la définition de l'association, chaque objet s'instancie indépendamment des autres, c'est-à-dire que chaque indice k,m ou n s'incrémente indépendamment. Ceci provient du fait que nous créons un espace à partir d'expressions décrivant des comportements sur des espaces indépendant. En d'autres termes l'expression X^{k+m+n} remplace une expression de la forme $X^k.Y^m.Z^n$ où X, Y et représentent les espaces respectifs des signaux signal1, signal2 et signal3.

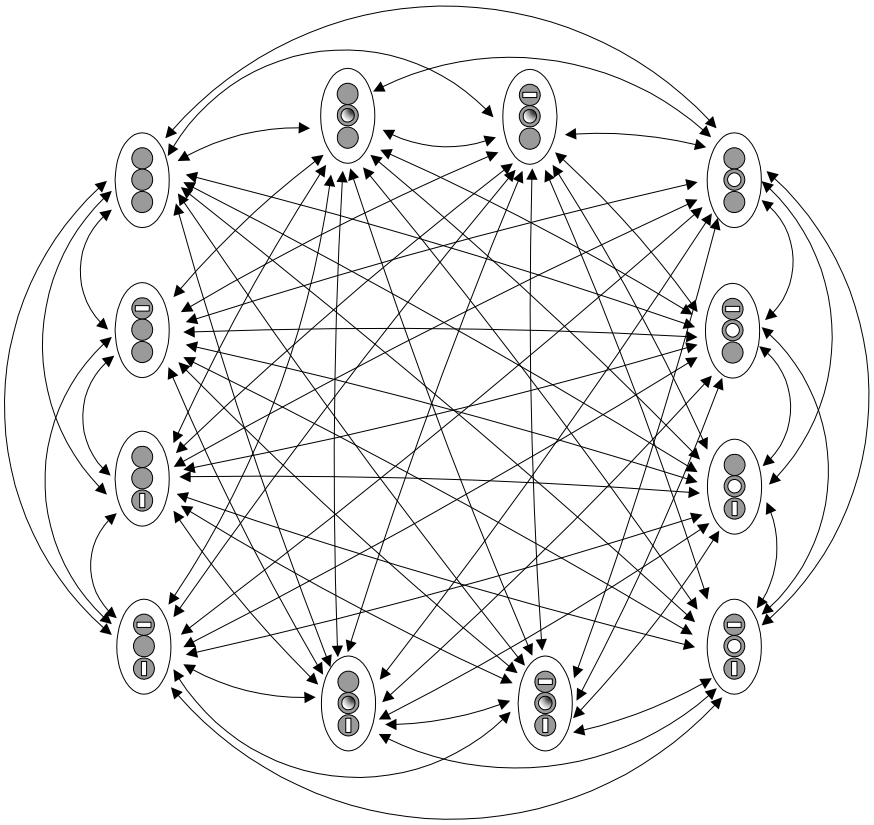


Figure 31 : graphe d'un feu vu comme une association de signaux

La simple association de propriétés telle que décrite ne restitue pas le fonctionnement du feu tel que nous le connaissons, à savoir, la mise en route par une phase clignotante et l'enchaînement des trois phases associées à l'autorisation de passage. En effet, dans la relation d'association les différents propriétés continue de s'instancier indépendamment, d'où l'écriture X^{k+m+n}. Ainsi pour définir le feu à partir de trois signaux il est nécessaire de définir la relation qui existe relation entre signal1, signal2 et signal3. Nous sommes en présence de la classe de relations de *partage* de *dépendance* et d'*influence*.

Prenons deux propriétés p[P, $\mathcal{P}$] et q[Q, $\mathcal{Q}$] quelconques, p[P, $\mathcal{P}$] en relation avec q[Q, $\mathcal{Q}$].

Dans la relation de *dépendance* la propriété q[Q, $\mathcal{Q}$] définira son comportement en fonction des réalisations de la propriété p[P, $\mathcal{P}$].

Dans la relation d'*influence* les réalisations de la propriété p[P, $\mathcal{P}$] induiront le comportement de q[Q, $\mathcal{Q}$].

Une relation de *partage* sous entend un échange, les réalisations des deux propriétés induisent mutuellement leur comportement.

En fait, ces trois types de relations matérialisent l'unité sémantique que représente un lien existant entre les réalisations de deux propriétés. Le partage, la dépendance ou l'influence ne sont que la représentation de l'orientation de ce lien. On peut alors exprimer une relation de ce type ainsi :étant donnés p[P, $\mathcal{P}$], q[Q, $\mathcal{Q}$] et z[Z, $\mathcal{Z}$] propriétés sur l'espace général Ω:

- z[Z, $\mathcal{R}$] est une relation de p[P, $\mathcal{P}$] et q[Q, $\mathcal{Q}$] si et seulement si p $\wedge$ z => q, on a alors une relation d'influence,
- z[Z, $\mathcal{R}$] est une relation de p[P, $\mathcal{P}$] et q[Q, $\mathcal{Q}$] si et seulement si q $\wedge$ z => p, on a alors une relation de dépendance,
- z[Z, $\mathcal{R}$] est une relation de p[P, $\mathcal{P}$] et q[Q, $\mathcal{Q}$] si et seulement si p $\wedge$ z <=> q $\wedge$ z, on alors une relation de partage.

A la différence des relations d'association et de généricité qui définissent un espace par la communauté de propriétés, les relations de partage, de dépendance et d'influence définissent un espace représentant une communauté de comportement de propriétés. Par communauté de comportement il ne faut pas entendre identité mais la définition d'un nouvel espace de réalisation induit par la relation. Compte tenu de la propriété d'endomorphisme de l'instanciation, il est évident que ces relations construisent non pas des nouveaux espaces de propriétés mais définissent des sous espaces de réalisation. Cette classe de propriété est donc créatrice d'un nouvel espace.

Examinons maintenant ces différentes relations à travers l'exemple du feu tramway. Son comportement peut se décrire sous la forme du graphe suivant :

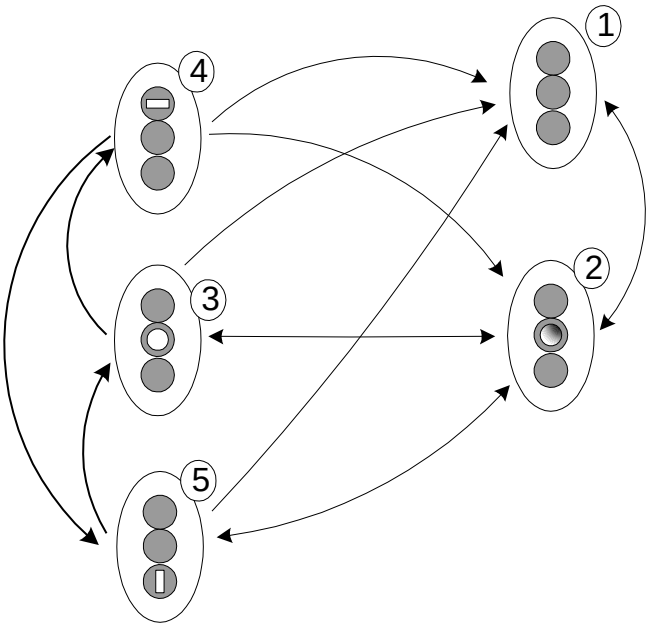


Figure 32 : graphe de comportement d'un feu tramway

Ce graphe correspond à l'expression de comportement suivante :

Feu(X) =

(

horizontal.éteint.disque.éteint.vertical.éteint+
horizontal.éteint.disque.clignotant.vertical.éteint +
(
horizontal.éteint.disque.éteint.vertical.fixe.X^0 +
horizontal.éteint.disque.fixe.vertical.éteint.X^1 +

horizontal.fixe.disque.éteint.vertical.éteint.X^2

).X^j

).X^i

Avec $i \geq 0$ et $j \geq 0$

La lecture de l'expression montre que le comportement du feu se décrit à partir d'un espace de réalisation et d'un sous espace de réalisation correspondant chacun à une propriété: fonctionnement et forme, s'instanciant individuellement mais non indépendamment.

Nous retrouvons là les deux propriétés de forme et fonctionnement utilisées précédemment pour décrire le feu. Ce sont ces deux propriétés qui définissent les relations décrivant le feu.

Nous avons noté que l'expression du comportement du feu conserve deux instanciation différentes ce qui nous a permis d'affirmer que l'espace objet feu est défini par la relations de deux propriétés des signaux, la forme et le fonctionnement.

Superposons ce graphe à celui de l'association des signaux :

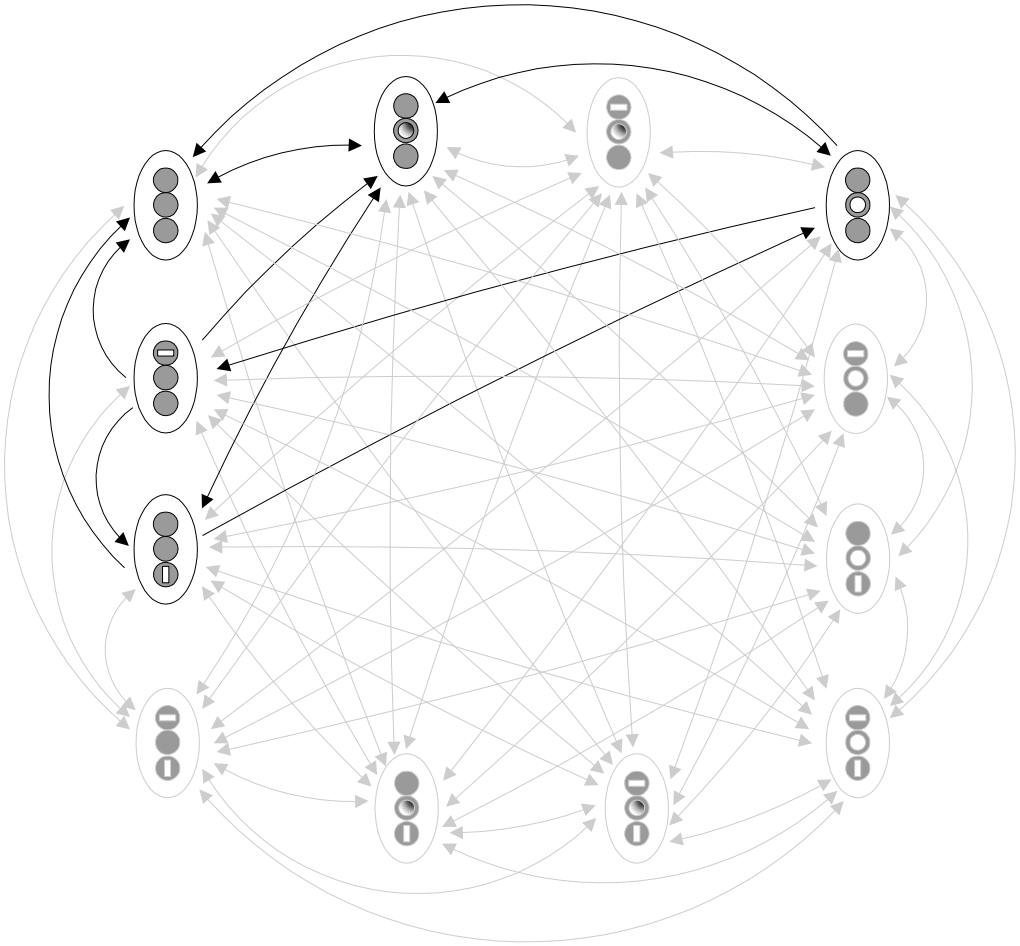


Figure 33 : graphe de l'espace de réalisation d'un feu tramway

On constate de façon évidente que tous les états de l'association ne sont pas utilisés, cette relation définit un sous espace de l'association.

La relation de dépendance entre propriétés est définie par le fait que toute réalisation de l'une implique la réalisation de l'autre. Donc la relation de dépendance entre deux propriétés définit un espace de réalisaiton décrit par la somme des comportements de chaque propriété.
Ici sur notre exemple, {horizontal.éteint.disque.éteint.vertical.éteint, horizontal.éteint.disque.clignotant.vertical.éteint, horizontal.éteint.disque.éteint.vertical.fixe, horizontal.éteint.disque.fixe.vertical.éteint, horizontal.fixe.disque.éteint.vertical.éteint} définit l'espace de réalisation du fonctionnement normal du feu.

A contrario, l'indépendance des propriétés implique l'indépendance des réalisations de ces propriétés. L'ensemble des évolutions de chaque propriété n'influe que sur le comportement de l'objet vis-à-vis de la propriété ; par conséquent, les $p_{n.}X^n$ et les $q_{m.}X^m$ sont indépendants, c'est-à-dire que les expressions de comportement q_mX^m seront considérés sous la forme d'une expression neutre $e.X^0$ vis-à-vis de l'espace de comportement défini par les expressions $p_{n.}X^n$ et réciproquement.

On vérifie bien que l'instanciation est une dimension du comportement d'un objet. Si un objet a des comportements multiples et indépendants, il y aura alors autant d'instanciations différentes.

Ainsi en ne considérant plus le feu comme une association de signaux de formes différentes mais comme un tout il est possible de simplifier l'expression décrite précédemment sous la forme suivante :

FeuTram(X) = (eteint + disque.clignotant + fixe.(vertical.X^j + disque.X^{j+1} + horizontal.X^{j+2})).X^i.

Pour écrire cette expression nous avons tout simplement posé que l'état éteint = horizontal.éteint.disque.éteint.vertical.éteint et choisi d'affecter $\in$ aux signaux éteints.

En écrivant cette forme simplifiée du comportement du feu nous avons pondéré sémantiquement certaines des expressions de comportement. Nous aborderons ce point particulier au chapitre 7 de ce mémoire.

De même, l'expression met en évidence un sous espace de réalisation lié à l'état fixe de la propriété fonctionnement du feu; c'est-à-dire que le comportement peut être décrit sous la forme du système d'expressions suivant :

FeuTram(X) = (eteint + disque.clignotant + fixe.forme(X)).X^i

Forme(X) = (vertical.X^j + disque.X^{j+1} + horizontal.X^{j+2})

EXPRESSIONS DE COMPORTEMENT, CHRONOLOGIE ET REFERENTIEL D'INSTANCIATION

La chronologie est une forme d'instanciation. En effet, la dynamique des espaces se décrit par un système bidimensionnel dimension complexe : instanciation – transformation. La transformation est la dimension de l'évolution d'un espace vis-à-vis de son environnement (y compris lui-même), une transformation d'un espace se traduit par l'apparition d'un système relationnel différent. L'instanciation est la dimension de l'action, elle rythme l'observation du comportement de l'espace. Elle se traduit par une application du domaine de définition de la propriété sur lui-même.

L'instanciation n'est pas le temps mais une forme de chronologie. Prenons par exemple une propriété quelconque p[P, $\mathcal{T}$] dont le comportement est décrit par l'expression suivante :

$P(X) = p_0X^n + p_1X^{n+1} + p_2X^{n+2}$.

Le terme *n* traduit alors la relation d'ordre entre les différents états de X introduite par le comportement de p[P, $\mathcal{I}$].

L'introduction d'une chronologie dans la description du comportement va correspondre à deux besoins différents pouvant être concomitants :

- la description d'un comportement continu,
- l'introduction d'un référentiel commun dans les expressions de comportement.

Pour la description d'un comportement purement continu, c'est-à-dire dont l'instanciation de la propriété n'est qu'une fonction du temps, l'expression du terme est de la forme : p_nX avec n = f(t). L'expression précédente deviendra alors par convention :

$P(X) = p_0X^t + p_1X^{t+\Delta t_1} + p_2X^{t+\Delta t_2}$ dans le cas d'une fonction discrète
ou
$P(X) = p_0X^{f(t)} + p_1X^{f(t)} + p_2X^{f(t)}$ dans le cas d'une fonction continue.

Quand il est nécessaire d'introduire un référentiel commun dans l'instanciation, on recherche en fait un plus petit commun multiple aux instanciations des propriétés dont la forme qui parait la plus évidente est le temps. Cependant, ce besoin peut intervenir sur des propriétés dont l'instanciation est indépendante du temps, il est donc indispensable de pouvoir définir un référentiel commun, non nécessairement temporel.

Reprenons l'expression de comportement du feu tramway suivante :

$FeuTram(X) = (eteint+disque.clignotant+fixe.(verticalX^j+disqueX^{j+1}+horizontalX^{j+2}))\ X^i$.

Nous voulons maintenant construire un croisement entre une voie de tramway et une voie routière, les deux à sens unique pour simplifier.

Nous pouvons simplement déduire l'expression de comportement du feu routier :

$Feu(X) = (off+yellow.blinking+fixed.(greenX^m+yellowX^{m+1}+redX^{m+2}))\ X^n$.

Nota: l'emploi de l'anglais ne se justifie que pour la clarté de ce qui va suivre.

D'après la définition de la relation de réalisation, l'expression de ce carrefour doit donc se définir comme un sous espace de l'association des deux espaces feux.

Nous avons vu dans les chapitres précédents de ce mémoire que les produits peuvent devenir assez rapidement lourds à manipuler.

Reprenons la forme système du comportement du feu tramway :

$FeuTram(X) = (eteint + disque.clignotant + fixe.forme(X))\ X^i$.

$Forme(X) = (verticalX^j+disqueX^{j+1}+horizontalX^{j+2})$.

Appliquons la au feu routier :

$Feu(X) = (off + yellow.blinking + fixed.Couleur(X))\ X^n$.

$Couleur(X) = (greenX^m+yellowX^{m+1}+redX^{m+2})$.

L'association des deux feux va donc se définir par le produit des deux systèmes d'expressions:

$FeuTram(X).Feu(X)$ = (eteint.off + eteint.yellow.blinking + eteint.fixed.Couleur(X) + disque.clignotant.off + disque.clignotant.yellow.blinking + disque.clignotant.fixed.Couleur(X) + fixe.Forme(X).off + fixe.Forme(X).yellow.blinking + fixe.Forme(X).fixed.Couleur(X)) X^{i+n}

A travers la mise en relation que nous venons de faire pour définir le carrefour, nous avons créé un espace commun. C'est-à-dire que l'expression X^{i+n} traduit l'instanciation unique des deux espaces feu tramway et feu routier $X^i.X^n$. Sachant que les conditions de fonctionnement d'un carrefour imposent que les feux soient dans le même état, éteints, fixes ou clignotant, on peut en déduire que la relation de réalisation du carrefour entre le feu tram et le feu routier se définit par la condition : i=n.

Le comportement du carrefour peut donc commencer par l'écriture d'une expression:

Carrefour(X)= (eteint.off+disque.clignotant.yellow.blinking+fixe.Forme(X).fixed.Couleur(X))X^k

avec k=i+n.

L'expression traduit bien que l'instanciation de l'espace carrefour est le résultat d'un changement d'état sur l'espace du feu routier et sur l'espace du feu tramway : le passage du carrefour éteint au carrefour en fonctionnement se fait par la transition conjointe des feux tramway et routier.

Nous venons donc de définir la relation entre les feux à partir d'un référentiel commun d'instanciation, ici l'identité, sur les espaces de réalisation individuels des deux feux. Il ne reste alors à définir la relation sur les sous espaces de réalisation décrits par Forme(X) et Couleur(X). Les conditions que nous voulons exprimer maintenant sont un peu plus complexes. Tout d'abord, nous définissons *ouvert un feu dont l'état est "vert" ou "jaune"; c'est-à-dire les valeurs vertical, green, disque et yellow*. Nous définissons fermé un feu dont l'état est "rouge"; c'est-à-dire les valeurs *horizontal* et *red*.

Les conditions de fonctionnement d'un carrefour peuvent s'exprimer simplement par le fait que les feux ne doivent pas être ouverts ensembles, et qu'il est nécessaire de maintenir une phase fermée intégrale avant chaque ouverture de feu.

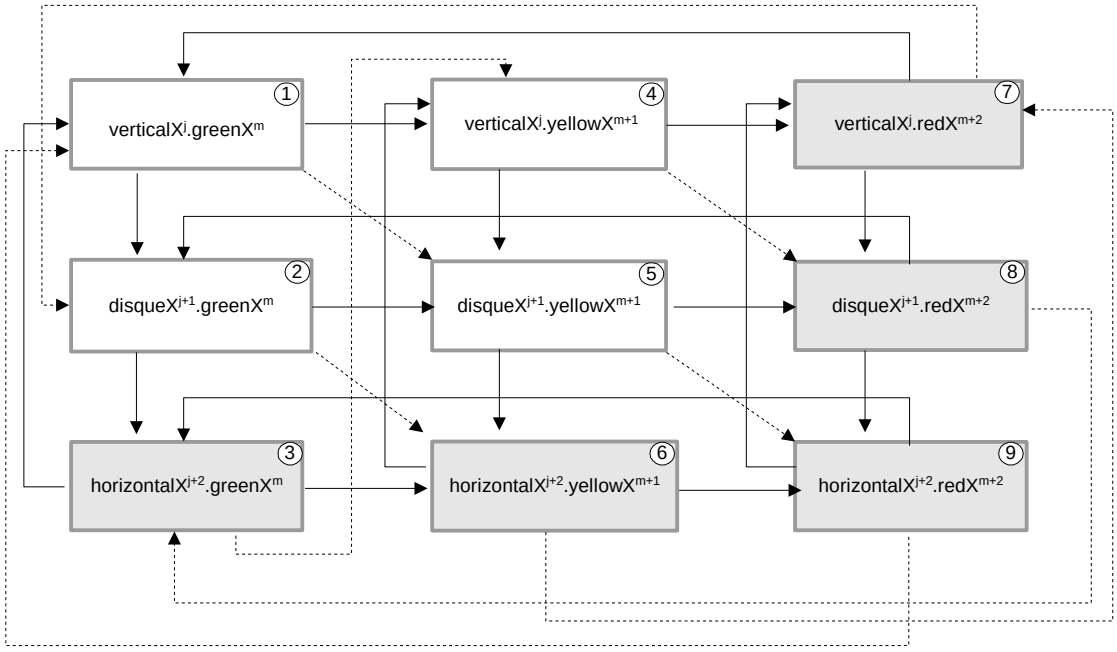
Pour démarrer le raisonnement, l'association fournit un sur espace de réalisation :

fixe.Forme(X).fixed.Couleur(X) =

fixe.(verticalX^j+disqueX^{j+1}+horizontalX^{j+2}).fixed.(greenX^m+yellowX^{m+1}+redX^{m+2}).

Etant donné que *fixe* et *fixed* sont des constantes dans ce cas précis, pour simplifier la suite de la démonstration nous allons raisonner uniquement sur les espaces décrits par Forme(X) et Couleur(X).

Examinons les graphes, les expressions de comportement et la matrice de l'espace de réalisation de l'association des espaces décrits par Forme(X) et Couleur(X) :



les flèches pleines indiquet une instanciation simple de m (horizontalement) et j (verticalement)
les flèches en pointillés indiquent une instanciation double (m et j)

Figure 34 : graphe global des états d'un carrefour

Ce graphe correspond à l'expression de comportement suivante :

Forme(X).Couleur(X) = verticalX^{j}.greenX^{m} + verticalX^{j}.yellowX^{m+1} + disqueX^{j+1}.greenX^{m} + **verticalX^{j}.redX^{m+2}** + disqueX^{j+1}.yellowX^{m+1} + **disqueX^{j+1}.redX^{m+2}** + **horizontalX^{j+2}.greenX^{m}** + **horizontalX^{j+2}.yellowX^{m+1}** + **horizontalX^{j+2}.redX^{m+2}**

L'expression que nous avons décrite ci-dessus donne le comportement du carrefour comme l'association de deux feux aux fonctionnements indépendants; c'est-à-dire sans aucune relation entre les valeurs de j et m. Les états pertinents ont été grisés sur le graphe et retranscrits en gras sur l'expression de comportement.

L'expression de l'espace du carrefour décrit par le comportement conjoint des deux feux devient :

vertical.redX^{k} + disque.redX^{k+1} + horizontal.redX^{k+2} + horizontal.greenX^{k+3}

+ horizontal.yellowX^{k+4} + horizontal.redX^{k+5}

Cette approche si elle décrit correctement le fonctionnement des deux signaux sur le carrefour ne reflète par le fait que l'espace du carrefour est le résultat d'une relation entre les deux espaces que sont les voies se croisant. Dans l'expression ci-dessus le carrefour est considéré comme un espace unique d'instance k = j+m. Il est donc plus pertinent de pouvoir conserver dans l'expression le fait que la relation porte sur la dépendance d'instanciation.

Revenons à notre exemple : on constate que le comportement souhaité du carrefour, instancie j puis m alternativement et inversement à partir de l'état fermé des deux voies – on parle de rouge intégral. Il existe une relation entre j et m, qui peut se décrire par des conditions d'instanciation de j et m par un simple algorithme :

Condition initiale : $m_0 = j_0 + 2$

Tant que $j \leq m$, incrémenter j

Tant que $m \leq j+2$, incrémenter m

Ce qui permet d'écrire l'expression du comportement du carrefour par l'expression suivante :

$(\text{vertical}X^{j}+\text{disque}X^{j+1}+\text{horizontal}X^{j+2}).\text{red}X^{m+2} +(\text{green}X^{m}+.\text{yellow}X^{m+1}+\text{red}X^{m+2}).\text{horizontal}X^{j+2}$

L'expression des espaces des relations de dépendance, ou relation de réalisation, est le point de la modélisation qui demande le plus d'attention. En effet, chaque relation crée un espace particulier dont la seule certitude que nous avons est qu'il est compris dans l'espace décrit par la relation d'association. La description qui va résulter de l'expression produite par le modélisateur va donc induire le comportement du modèle final. Pour cette raison, il vaut mieux considérer une relation de dépendance comme une propriété indépendante sur l'instanciation.

CONCLUSION

Nous venons à travers ce chapitre de définir tous les éléments sur lequel est fondé le modèle de représentation. En premier lieu, nous avons défini la notation d'une propriété p[P, $\mathscr{I}$] comportant un identifiant p qui peut dans le cas d'une propriété dynamique être considéré comme une variable, P le domaine de définition et surtout $\mathscr{I}$ l'unité sémantique permettant de manipule la propriété comme un élément du langage. Nous avons complété cette expression en montrant qu'il est qu'il est possible de définir n'importe quel comportement comme la somme d'expression rationnelles de propriétés sur l'espace général Ω. Toute propriété est une expression rationnelle de ses parties finies, celles-ci étant représentées par des propriétés élémentaires, des associations de ces propriétés, et par l'union de leurs espaces de réalisation.

Nous avons ensuite montré l'existence d'un morphisme de l'espace des expressions rationnelles (Ω, +, . , *, ∈) dans (Ω, +, .) qui permet de définir $A(X) = \sum_{i=0}^{i=t} p_i X^i$ une forme algébrique de ces expressions rationnelles comme l'évolution de l'espace X relativement au comportement A de la propriété p[P, $\mathscr{I}$]. Nous avons rapproché cette forme de représentation des comportements des différents types de relations qui peuvent être établies entre les propriétés, de l'association jusqu'au relations de dépendance, en particulier les relations fondées sur une interaction de la chronologie des instanciations.

La définition donnée d'une propriété p[P, $\mathscr{I}$] permet de caractériser les évolutions d'un espace quelconque de propriétés à travers sa relation avec les réalisations de ses propriétés. Le choix du système d'écriture formel d'une propriété associant sémantique et valeurs des réalisations permet de ne pas perdre le couplage avec le langage lors de la transposition du comportement vers l'expression rationnelle. Enfin, nous avons montré à partir de la définition d'un élément neutre que la modélisation proposée est en fait l'image d'un morphisme de l'espace observable vers un espace observé et ainsi que l'information non utilisée n'est en aucun cas "oubliée", ce qui autorise le modélisateur à ne s'intéresser qu'à l'information utile.

MODELISATION ET REPRESENTATION

INTRODUCTION

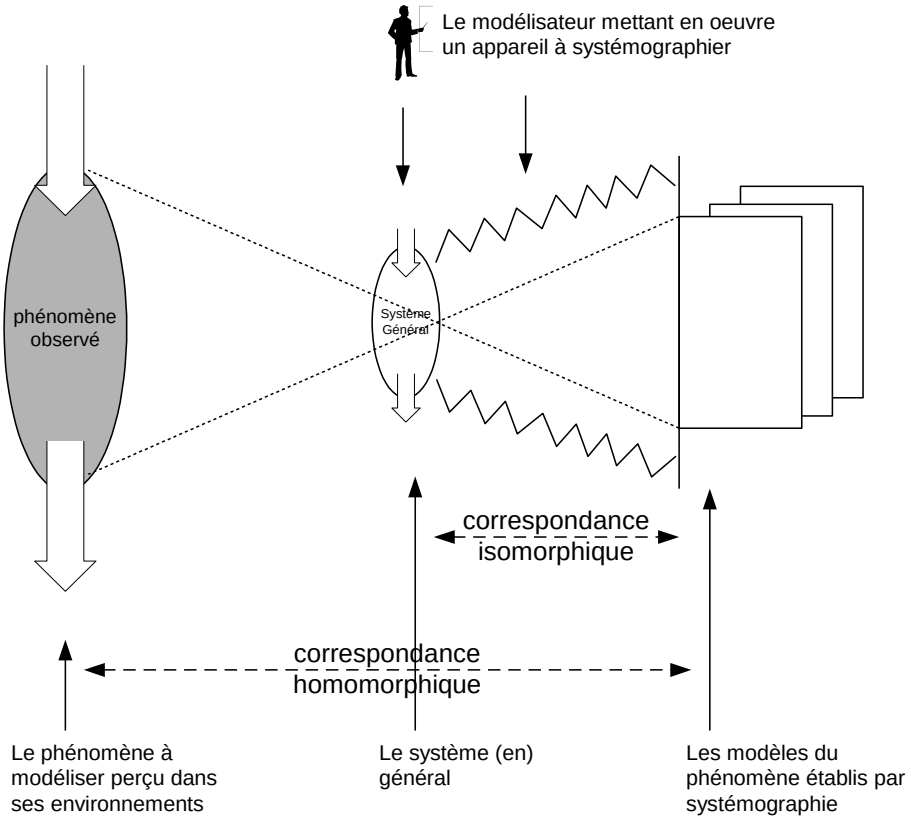
Nous venons de définir un modèle de représentation permettant de manipuler les propriétés et leurs comportements minimisant l'effet de la transformation, ceci grâce à l'utilisation des unités sémantiques. Cette approche modélisatrice permet de considérer un système non pas par sa structure mais à partir de ses projets. L'utilisation du concept de propriété dans la représentation du système autorise une description des comportements et permet la modélisation de l'organisation visant à achever ces projets. Or, un des objectifs de cette recherche est de permettre une modélisation d'éléments technologiques mais aussi des aspects humains et connaissances qui accompagnent le fonctionnement de celui-ci.

Si l'utilisation de ces concepts et du modèle de représentation associé peut apparaître immédiate dans la modélisation d'un système simple, il devient difficile de décrire directement les propriétés qui caractérisent un système complexe. En particulier, le premier critère de complexité est lié à la prise en compte du facteur humain et des représentations conceptuelles à partir desquelles le cerveau établit ses raisonnements.

Il convient donc de compléter ce modèle par une approche plus macroscopique et plus méthodologique dans l'appréhension d'un système à des fins de modélisation. Nous allons utiliser un modèle de système général qui constitue un point d'entrée plus universel vers le modèle de représentation. Ce modèle de système général fournira une vision macroscopique d'un système quelconque permettant d'appréhender simplement les relations entre les différents intervenants et quelle est leur nature respective.

LA VISION SUR LE MONDE REEL : LE SYSTEME GENERAL

Cette notion de système général est développée par J.L. Le Moigne qui préconise dans [LE MOIGNE 1990] la modélisation par systémographie; c'est-à-dire en représentant le système à modéliser comme et par un système général. En modélisation par systémographie, le concept de système général agit un peu comme une "lentille de télescope" (SIC) en produisant une représentation homomorphique du système réel. En revanche la transformation du système observée n'est effectuée qu'à cette étape la suite de la modélisation restant isomorphe à ce modèle général.



Mode d'emploi :

cadrage : construction d'un modèle par isomorphie avec le système général.

développement : documentation de ce modèle par correspondance homomorphique avec des caractéristiques du phénomène perçu.

Interprétation : Simulation d'actions possibles sur le modèle pour anticiper les conséquences éventuelles dans le phénomène.

Figure 35 : La systémographie d'après J.L. Le Moigne

A travers cette approche le système général agit comme un modèle conceptuel unifié qui permet de construire une représentation du système en prenant en compte l'organisation, la mise en relation et l'articulation de structures pour en faire émerger un comportement complexe. En fait, en définissant un système général nous établissons un méta modèle descriptif de n'importe quel système. Le système général conceptualise et représente un espace type dont l'organisation doit respecter une structure représentative de n'importe quel système ou de n'importe quelle organisation. Il sera ainsi possible de décliner toute partition ou tout sous espace de cet espace initial sous la même forme.

Pour la description d'un système, une représentation systémique repose sur seulement trois niveaux logiques :

- les environnements du système,
- le système en lui-même, à partir de ses frontières,
- ses composants internes (sous-systèmes ou processeurs).

Cependant l'approche systémique n'entre a priori pas dans l'analyse des processeurs eux-mêmes. S'il est nécessaire d'approfondir la connaissance des processeurs ceux-ci sont à leur tour considérés comme des systèmes dont leur extérieur respectif constitue l'environnement. J.L Le Moigne, propose la définition d'un système général comme une collaboration entre un système opérant, qui transforme les flux intrants en flux extrants, un système de décision (ou de pilotage) et un système de connaissances. Cette représentation trouve son origine dans la modélisation de systèmes décisionnel et organisationnel à composante humaine prépondérante. L'approche systémique ayant surtout pour finalité l'observation de système complexes comme des organisations humaines, ce modèle, appelé modèle OID, permet de définir un modèle matriciel de représentation de l'organisation d'un système avec en colonne la représentation structurelle du système général et en ligne la dynamique d'action.

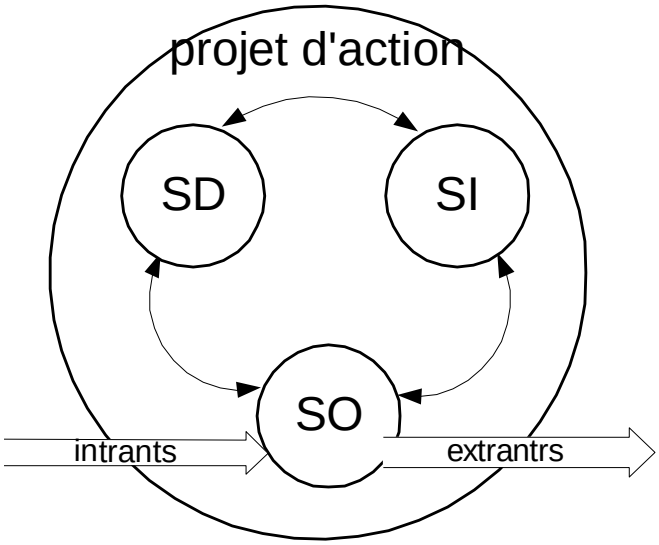


Figure 36 : modèle OID

Pour ce modèle, un projet d'action se définit comme la combinaison d'un acquis (les comportements passés), d'un présent (les sollicitations de l'environnement), et d'un futur (les intentions d'actions avec leurs conséquences telles qu'elles sont anticipées par le système). Dans cette représentation du système général, les flux entrants et sortants représentent tout ce qui intervient dans le projet d'action sans en faire partie. On s'aperçoit aisément qu'un projet d'action évolue en fonction de l'enrichissement de son système d'information, c'est-à-dire que celui-ci s'enrichit des intrants ou du feedback sur les extrants. Un projet d'action ne peut donc être déterminé qu'à un instant donné. De même, l'environnement est alors perçu comme un flux entre deux systèmes ou la conséquence d'un flux sur un système sur les autres systèmes en relation (champ). L'environnement n'apparaît donc pas comme un objet de l'espace mais comme la mise en situation d'un projet d'action.

Cette représentation OID est intéressante car elle postule qu'un système quelconque peut être considéré comme la collaboration d'un intervenant actif (opérateur décisionnel du système), d'objets opérants et d'un référentiel de connaissance (utilisation, architecture, domaine technique d'application…), certains parties étant alors vide ou sans influence.

PROPRIETE ET SYSTEME GENERAL

Nous avons établi précédemment qu'une propriété, et par extension un espace de propriétés, se définissaient par un domaine de définition et une représentation sémantique. Par exemple, si nous considérons un système construit autour d'un interrupteur, le système opérant sera l'interrupteur, le système d'information manipulera l'unité sémantique *interrupteur* et le système de décision manipulera les propriétés de l'interrupteur et l'unité sémantique *interrupteur*. Si nous mettons cet objet en situation le système opérant va établir des relations sur le domaine de définition de l'objet interrupteur (l'espace de la réalité physique), indépendamment du nom ou unité sémantique représentant l'interrupteur. En d'autres termes, si nous manipulons un interrupteur nous manipulons la propriété de cet objet, mais pas un concept représentatif. Par contre, lorsque nous décidons d'utiliser la propriété de l'interrupteur, nous formons un raisonnement établissant un projet d'action à travers un réseau de relation mettant en œuvre une représentation conceptuelle de la propriété de l'interrupteur. Cette représentation conceptuelle s'appuie sur un langage (unités sémantiques) pour décrire la propriété: cette représentation conceptuelle est l'espace de la connaissance. On s'aperçoit alors qu'un système articulé autour de l'interrupteur met en œuvre trois espaces représentatifs d'une même chose : l'espace de l'objet lui-même, l'espace représentant la connaissance de cet objet, et l'espace de l'utilisateur/décideur.

Le modèle de système général postule qu'un système n'est pas un simple objet mais la combinaison d'au moins trois espaces : l'espace de la réalité physique, l'espace de la connaissance, l'espace de la décision. Il faut noter que ce modèle ne propose pas une structure générique de l'organisation d'un système, mais l'image naturelle de l'organisation d'un système établie à partir du mode sur lequel s'établissent les relations entre ses propriétés. On peut aussi parler d'une différenciation établie à partir du point de vue suivant lequel est appréhendée la propriété : réalité, connaissance, projet d'action. Nous pouvons alors proposer la construction d'une représentation du modèle de système général en fonction des relations sur les propriétés :

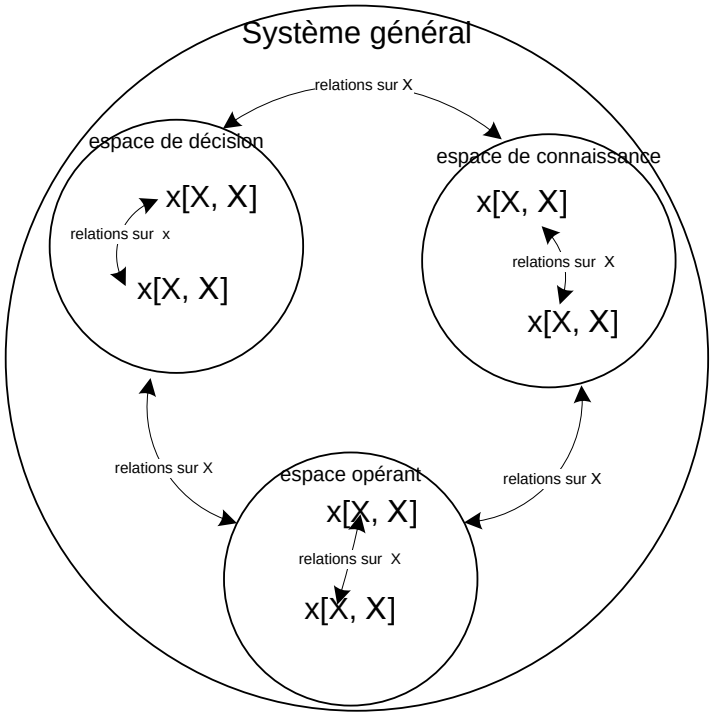


Figure 37 : modèle général Espaces - processus

Ce modèle exprime que le système est appréhendé le plus généralement possible comme la mise en relation d'un espace technique, d'un espace régulateur ou documentaire et d'un espace humain. Le système idéal, devrait donc garantir une parfaite isomorphie entre ces trois espaces, ce qui, bien sûr, reste pure utopie. Pour bien comprendre ce modèle et ce qu'il représente nous allons aborder cet aspect de la modélisation à travers deux exemples :

- L'exemple du carrefour, qui dans la continuité de ce mémoire va permettre de montrer comment se mettent en place les aspects technologiques, documentaires et humain du modèle;
- L'exemple du contrôle d'un aérodrome qui nous permettra d'aborder un système essentiellement régulateur.

MODELISATION D'UN SYSTEME OPERANT

Dans ce paragraphe nous allons considérer la description technique d'un carrefour en croix, sans traversée piéton. L'utilisation du modèle général suppose que le système à modéliser est défini par un projet ; c'est le point de vue systémique. En d'autres termes, le modèle ne doit pas aborder le carrefour, suivant des points de vues comme :

- le point de vue géographique : le croisement de deux voies vu comme l'association de deux espaces,
- le point de vue technique : la gestion de deux flux par un même contrôleur au moyen de signaux.

Donc la première démarche dans l'appréhension du modèle est : quel est le projet ?

La propriété d'un carrefour étant le croisement de trajectoires antagonistes, nous pouvons poser que le projet du carrefour est donc de permettre le croisement des flux de véhicules en évitant les collisions. Pour cela, les conducteurs doivent obéir à une signalisation particulière qui décide qui peut ou pas passer suivant les différentes configurations de la circulation. Nous venons en quelques mots de définir le modèle général d'un carrefour comme :

- un espace de décision : les conducteurs,
- un espace opérant : la signalisation,
- un espace de connaissance : le code de la route.

Ce modèle général est valable quelque soit le mode choisi pour gérer le carrefour : feux, panneaux, pas de signalisation. Le projet a donc défini le modèle général. A partir de ce modèle général, nous pouvons maintenant affiner la connaissance des trois espaces.
La question qui se pose ensuite est : par lequel commencer ?
La réponse est par l'espace qui définit le projet.
Les véhicules, et par voie de conséquence, les conducteurs représentant les flux processés par le système, et la signalisation le moyen de les gérer. La réponse est donc naturellement par l'espace de connaissance. Cette réponse trouve une justification naturelle dans le fait que la connaissance est l'interface entre le système opérant qui dans le cas présent est perçu par le conducteur et la décision qui va découler de l'interprétation du signal. Attention, suivant le projet la réponse n'est pas forcément la même; Si nous voulons modéliser un système en vue de déterminer quels en sont les éléments de conduite, nous commencerions par l'espace opérant ; par exemple, lorsqu'on établit le manuel de vol d'un aéronef. De même, la détermination de l'ergonomie d'un système (interface homme machine) est l'exemple d'une modélisation s'appuyant sur l'espace opérant.

Dans notre exemple, l'espace de connaissance est un espace régulateur, car il contraint le fonctionnement du système.
Le code de la route définit trois règles principales de croisement de véhicules qui peuvent se résumer ainsi :

- le passage contrôlé : les flux de véhicules sont gérés par des feux,
- le passage protégé : le véhicule sur la voie prioritaire passe, le conducteur sur la voie secondaire ne peut passer qu'en s'assurant qu'aucun véhicule n'arrive sur la voie prioritaire,
- le régime de la priorité à droite : laisser passer le véhicule arrivant par la droite.

Nota : même si nous avons identifié un espace conducteur, nous parlons de véhicule, car les véhicules constituent les flux processés par le système. Chacune de ces trois règles implique un système opérant particulier :

- le passage contrôlé : une signalisation dynamique,
- le passage protégé : une signalisation permanente,
- la priorité à droite : aucune signalisation.

Ces trois règles respectent la hiérarchie suivante : passage contrôlé puis passage protégé puis priorité à droite.

Nous devons donc maintenant représenter trois espace de propriétés représentant ce que nous venons succinctement de définir.

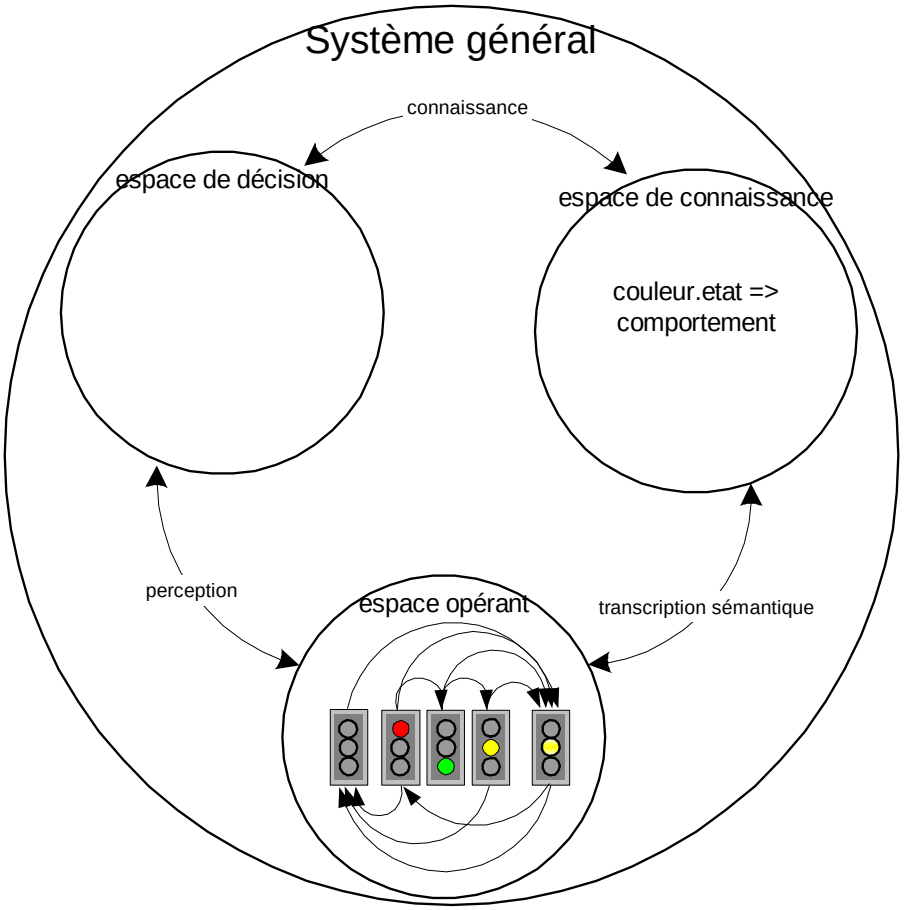


Figure 38 : modèle général simplifié d'un carrefour

Pour représenter le modèle général du carrefour, nous allons maintenant utiliser la définition complète d'une propriété, à savoir valeur, domaine de définition, unité sémantique. En effet, si valeur et domaine de définition constituent les éléments constitutifs de la propriété et de son comportement, l'unité sémantique en est la représentation intellectuelle. Par exemple, la couleur rouge du signal est sur un carrefour chargé d'une signification précise et correspond à un ordre d'arrêt. L'espace de connaissance peut se résumer ainsi :

- signal rouge : arrêt obligatoire,
- signal jaune : stopper si possible,
- signal vert : passage autorisé,
- signal jaune clignotant : application du régime suivant.

Il est intéressant alors d'écrire les propriétés caractéristiques des signaux sous la forme suivante :

- rouge[{rouge},"stopper"],
- jaune[{jaune}, "stopper si possible"],
- vert[{vert}, "passer"],
- clignotant [{clignotant},"autre régime"]
- eteint [{eteint}, "autre régime"]

Ce qui se traduira sur le modèle général par une relation sémantique entre les espaces de décision et de connaissance – relation assez naturelle – et par une relation d'instanciation entre l'espace de décision et l'espace opérant.

En considérant j et m les deux voies antagonistes comme deux espaces de réalisation s'instanciant indépendamment, et k l'espace commun d'instanciation, l'expression de comportement des feux sera la suivante :

$$Carrefour(X) = (eteint.eteint + clignotant.clignotant + (vert.X^{j}+jaune.X^{j+1} + rouge.X^{j+2}).rouge.X^{m+2} + (vert.X^{m} + jaune.X^{m+1} + rouge.X^{m+2}).rouge.X^{j+2}).X^{k=2j=2m}$$

Nous n'avons abordé jusque là que l'élément technique du carrefour; envisageons maintenant l'aspect humain à travers l'espace de décision. Nous avons d'une part définit les différents connaissances associées au carrefour par l'association de caractéristiques et d'unités sémantiques; nous avons d'autre part définit le fonctionnement des signaux du carrefour de façon à éviter toute circulation antagoniste. Dans ses aspects techniques, l'espace de décision du carrefour va donc correspondre à l'action que doit effectuer le conducteur, élément du flux processé par le système carrefour.

L'espace de décision est principalement caractérisé par une propriété décision[{stopper, passer},"décision"]. Stopper et passer étant les réalisations des propriétés élémentaires passer[{passer}, "passer"] et stopper[{stopper}, "stopper"]. D'après le modèle général que nous avons défini précédemment la propriété décision[{stopper, passer},"décision"] n'est en fait qu'une relation établie sur la valeur de la propriété feu perçue par le conducteur et l'interprétation qu'il doit en faire, c'est-à-dire la connaissance qu'il a des signaux. Dans l'espace de connaissances, l'expression définissant le comportement des flux de véhicules pourrait être directement déduit de l'expression de comportement du système opérant et des propriétés de l'espace de connaissance:

$$("autre régime"."autre régime"+ "autre régime"."autre régime" +$$

$$(("passer".X^{j}+"stopper si possible".X^{j+1}+"stopper".X^{j+2})."stopper".X^{m+2} +$$

$$("passer".X^{m}+."stopper si possible".X^{m+1}+"stopper".X^{m+2})."stopper".X^{j+2}).X^{k}$$

Or, l'espace de connaissance présente une valeur de propriété "stopper si possible" ne correspondant pas à une valeur différenciée de la propriété décision[{stopper, passer},"décision"]. En d'autres termes, cette valeur de la propriété du feu va pouvoir correspondre à la fois à la valeur stopper et à la valeur passer. Sachant que l'expression de la propriété décision s'écrit (passer + stopper).X^{i}, l'expression de la décision d'un conducteur sur un axe de circulation en fonction de l'état du feu sera de la forme :

$$(vert.passer.X^{i}+(stopper + passer).jaune.X^{i+1}+ rouge.stopper.X^{i+2})$$

Et l'expression de la décision des conducteurs sur un carrefour :

(

(stopper + passer).eteint.(stopper + passer).eteint +

((stopper + passer).clignotant.((stopper + passer).clignotant +

(vert.passer)).X^j + (stopper + passer).jaune.X^{j+1} + rouge.stopper.X^{j+2}).rouge.stopper.X^{m+2} + (vert.passer.X^m+(stopper + passer).jaune.X^{m+1}+ rouge.stopper.X^{m+2}).rouge.stopper.X^{j+2}).X^k

Nous remarquons que l'expression exprime le fait que nous construisons un espace conducteur - feu dont le conducteur est l'espace de décision, le feu l'espace opérant et l'expression l'espace de connaissance mais aussi que le carrefour est un espace plus complexe constitué d'espaces conducteur - feu mais aussi conducteur – carrefour. La variable X^k signifiant que nous avons un espace commun, et chaque variable X^j et X^m représentant l'espace de chaque axe de circulation. Reprenons l'expression du carrefour et développons-la :

eteint.eteint.X^k + clignotant.clignotant.X^k + ((vert.X^j+jaune.X^{j+1}+rouge.X^{j+2}).rouge.X^{m+2}).X^k+ (vert.X^m+.jaune.X^{m+1}+rouge.X^{m+2}).rouge.X^{j+2}).X^k

Si nous considérons le fonctionnement cyclique du feu et développons ces termes nous aurons respectivement :

- ((vert.X^j.rouge.X^{m+2}+jaune.X^{j+1}.rouge.X^{m+2}+rouge.X^{j+2}.rouge.X^{m+2}).X^k
- (vert.X^m.rouge.X^{j+2}+.jaune.X^{m+1}.rouge.X^{j+2}+rouge.X^{m+2}.rouge.X^{j+2}).X^k
- Sur l'espace de décision ces expressions s'écrivent :
- ((vert.passer.X^j.rouge.stopper.X^{m+2} + jaune.passer.X^{j+1}.rouge.stopper.X^{m+2} + jaune.stopper.X^{j+1}.rouge.stopper.X^{m+2} + rouge.stopper.X^{j+2}.rouge.stopper.X^{m+2}).X^k,
- ((vert.passer.X^m.rouge.stopper.X^{j+2} + jaune.passer.X^{m+1}.rouge.stopper.X^{j+2} + jaune.stopper.X^{m+1}.rouge.stopper.X^{j+2} + rouge.stopper.X^{m+2}.rouge.stopper.X^{j+2}).X^k

Nous constatons que nous n'avons jamais pour une même instance une décision de passer sur les deux voies.

En revanche, si nous considérons les états éteint ou clignotant du carrefour, l'expression de la propriété décision[{stopper, passer},"décision"] devient :

- (eteint.stopper.eteint.stopper + eteint.stopper.eteint.passer + eteint.passer.eteint.stopper+eteint.passer.eteint.passer).X^k
- (stopper.clignotant.stopper.clignotant + stopper.clignotant.passer.clignotant + passer. clignotant.stopper.clignotant + passer.clignotant.passer.clignotant).X^k

On constate aisément qu'aucune règle issue des espaces précédemment décrits ne régit le carrefour. Nous venons de montrer à travers ce chapitre que le modèle général à trois espaces décision – opération – connaissance ne correspondait pas à une simple recopie des propriétés de l'un sur l'autre mais à la création d'un espace complexe à travers des relations :

- physiques : relations de l'espace opérant avec l'espace opérant,
- connaissance : relations de l'espace de connaissance avec l'espace de décision,
- sémantique : relation de l'espace opérant avec l'espace de connaissance.

Le modèle général correspond bien à un espace général représentatif sur lequel on retrouve la chose, la connaissance que nous en avons et ce que nous en faisons.

MODELISATION D'UN ESPACE DECISIONNEL ASSOCIE

Le modèle établi précédemment permet d'identifier les espaces par lesquels se définit le carrefour. Cependant, on constate que la décision de chaque conducteur est l'élément clé dans l'occurrence d'une collision et qu'il est nécessaire de compléter l'expression de comportement de la propriété décision[{stopper, passer},"décision"] par des relations avec d'autres propriétés de l'espace opérant. Si nous considérons n'importe quel objet technique nous constatons qu'il agit (ou réagit) toujours suivant le même principe : Sans énergie et sans entrée, il n'y a production d'aucune sortie. Dans le cas de l'être humain, sa capacité créatrice implique que sa simple présence dans l'environnement d'un système en fait un acteur du comportement de celui-ci.

Intéressons nous à la phase de fonctionnement normal d'un feu routier, sous sa forme sémantique :

$$\text{"passer"}X^{j} + \text{"stopper si possible"}X^{j+1} + \text{"stopper"}X^{j+2}$$

Cette expression correspond au comportement souhaité d'un conducteur en présence d'un feu. Dans le chapitre précédent nous avons considéré l'espace de décision du carrefour en partant d'un monde idéal dans lequel chaque conducteur appliquait les règles du code de la route. En fait l'espace de décision décrit est celui de la décision attendue or la particularité des systèmes à composante humaine est la forte individualité et la forte créativité des comportements. Cependant, ceci ne remet pas en cause le modèle du carrefour, c'est l'un des principaux intérêts de l'approche proposée. Ceci se traduit par le fait que pour certaines phases du fonctionnement du carrefour le comportement des véhicules ne peut plus être considéré systématique mais s'individualise fortement. Remarquons que dans une approche purement espaces, nous sommes obligé de considérer le carrefour dans son ensemble, si nous passons en approche proposée espaces - processus, nous avons alors pour un même espace général du carrefour des espaces instanciés dont certains offrent un comportement stable et par conséquent systématique et d'autres un comportement moins systématique. Nous retrouvons les phases stables du fonctionnement du feu (signaux au vert et au rouge) le comportement des véhicules correspond au comportement attendu alors que pendant les phases de transition le comportement des conducteurs s'individualise fortement. On observe cette individualisation pendant :

- les phases de transition, c'est-à-dire les phases de jaune, voire de début de rouge dans certaines villes ou certains pays,
- les phases où la consigne est moins impérative comme le jaune clignotant, ou chacun franchi le carrefour suivant son interprétation ou sa connaissance du code de la route.

Le constat que nous faisons de l'individualité de la décision peut se traduire sur notre modèle par l'existence d'un système particulier qui par l'occurrence d'un événement "arrivée sur le carrefour" dévient partie de l'espace de décision du système carrefour. En application du principe de modélisation que nous avons retenu, ce système est alors composé lui-même d'un espace opérant, d'un espace de connaissance et d'un espace de décision. La représentation du modèle général devient alors la suivante :

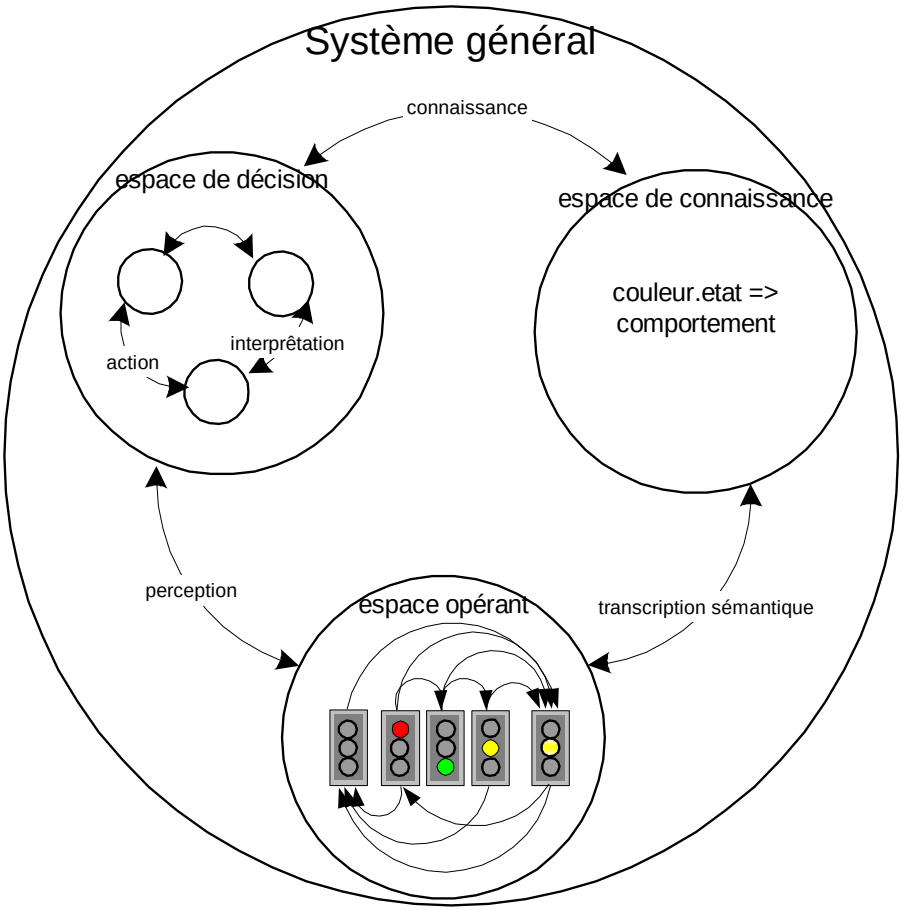


Figure 39 : modèle général d'un carrefour

Le modèle général du carrefour exprime le fait que nous construisons un espace véhicule - feu dont le véhicule est l'espace de décision, le feu est l'espace opérant et l'expression de comportement définit l'espace de connaissance, mais aussi, que le carrefour est un espace plus complexe constitué aussi d'espaces conducteur – carrefour.

Ce dernier point est intéressant car dans la définition générale du modèle l'espace opérant du conducteur contient une image de l'espace opérant du feu, par contre pour une instance particulière de cet espace l'espace opérant du conducteur contient l'image d'une réalisation du feu. En d'autres termes, le modèle de l'espace opérant du conducteur contiendra dans son expression générale l'expression de comportement du feu – vert.X^m+.jaune.X^{m+1}+rouge.X^{m+2}- alors qu'une instance donnée se traduira par une instance couleurX^m.

De même, l'espace de connaissance du conducteur contiendra l'expression du carrefour :

eteint.eteint.X^k + clignotant.clignotant.X^k + ((vert.X^j+jaune.X^{j+1}+rouge.X^{j+2}).rouge.X^{m+2}).X^k+ (vert.X^m+.jaune.X^{m+1}+rouge.X^{m+2}).rouge.X^{j+2}).X^k

Si à partir d'un modèle de décision nous décidons de l'appliquer au modèle du carrefour, il s'établit instantanément un couplage entre l'espace opérant et espaces de connaissance.

Nous constatons aussi que la structure du modèle général se reproduit dans les deux sens macro vers micro modélisation et micro vers macro modélisation. Il est ainsi possible d'aborder un problème depuis n'importe quel point de vue sans remettre en question le modèle de représentation.

Appliquée au modèle humain, le système de décision "conducteur" est donc composé d'un espace opérant – perception et action- d'un espace de connaissance – mémoire – et d'un espace de décision. Ce modèle humain très sommaire reprend pourtant la représentation du système de décision humain tel qu'il est représenté dans différents travaux.

En dehors des aspects connaissances, intelligence et sensibilité, le comportement humain se caractérise par sa capacité d'initiative et sa réponse aux émotions. Antonio DAMASIO (directeur du département neurologique de l'université de l'Iowa) a fait le constat expérimental [DAMASIO99] que deux mécanismes sont à l'œuvre dans le processus de prise de décision. D'une part la voie de la raison utilise les connaissances et la logique. D'autre part, un mécanisme par lequel l'émotion rétrécit le champ de décision, simplifie la tâche de la raison. Damasio postule que le souvenir des émotions passées, réactivées par un circuit neuronal qui prend en compte les modifications corporelles liées à l'émotion va ainsi influencer et marquer la décision finale en activant l'attention sur les conséquences à venir en interférant avec la raison. Ces marqueurs sont issus de notre mémoire émotionnelle qui crée peu à peu des catégories (joie, deuil…) reliant l'image d'objets ou d'évènements avec des états corporels (somatiques) plaisants ou déplaisants. Le rappel des informations contenues dans ces marqueurs peut être conscient ou inconscient.

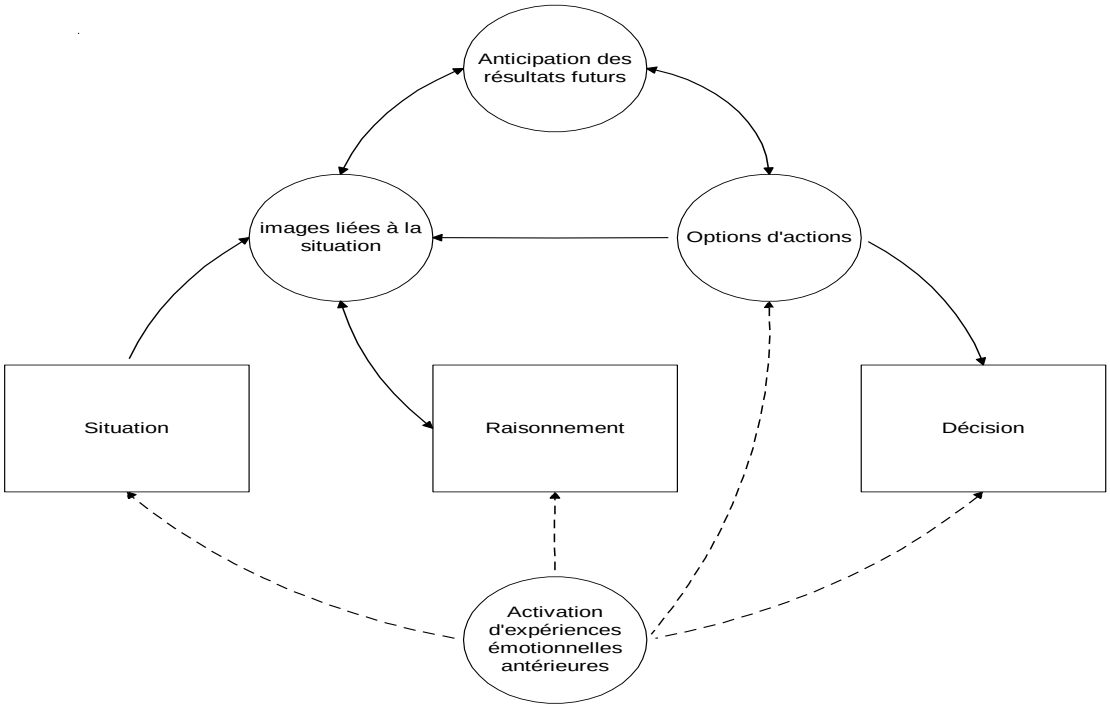


Figure 40 : modèle de DAMASIO du système humain

L'humain ne peut donc être considéré comme un simple système réactif, ou de prise de décision logique, quoiqu'une bonne formation tende à réaliser ce dernier objectif. Il devient donc difficile de définir un modèle générique de prise de décision. Il n'est évidemment pas question de reproduire un modèle ou un autre qui fait appel à des mécanismes émotionnels complexes. Par contre, le propos de Damasio met en évidence que le système humain doit voir le modèle de raisonnement basé sur la connaissance et la logique enrichi par un système concurrentiel parallèle, lié à l'expérience. Nous retrouvons là, les composantes de notre modèle général :

- Un système opérant : perception, exécution.
- Un système de connaissance : mémoire, savoir, expérience.

- Un système de décision : logique, émotions, objectifs.

Le propos de ce mémoire n'est pas d'aborder la modélisation de l'esprit humain mais de monter qu'il est possible à travers l'approche proposée de coupler un modèle ou une autre sans remettre en question, le modèle général du système sur lequel on choisit de travailler.

Dans un premier temps on peut constater que si on considère le système complet carrefour conducteur du point de vue du carrefour, nous aboutissons alors à un modèle général traduisant un couplage entre les systèmes :

- l'espace opérant défini un espace de connaissance associé qui en est l'image sémantique.
- L'espace de décision intègre un espace de la perception du carrefour, et un espace de la connaissance qu'a le conducteur du carrefour.

APPREHENSION DU SYSTEME GENERAL : EXEMPLE DE LA CTR

Pour mieux comprendre l'intérêt de ce modèle, sortons provisoirement de notre carrefour routier.

Nous allons montrer dans un premier temps qu'il peut rapidement apparaître une confusion entre une approche espaces-processus et une illusion d'approche espaces-processus puis ensuite montrer comment simplement l'appliquer.

Nous allons procéder à une approche erronée en partant du principe que le modèle peut se déterminer soit par ses processus soit par ses espaces. Etant donné que l'approche par processus est très semblable à une démarche fonctionnelle, nous allons tenter de déterminer le modèle général à partir des espaces. Pour identifier ces espaces nous allons identifier les relations entre les principaux objets du système en partant du principe que chacune construit un nouvel espace.

Prenons pour exemple la gestion des circulations des aéronefs sur un aérodrome contrôlé, ou gestion d'une CTR. L'intérêt principal de ce système est que même s'il met en œuvre essentiellement des objets techniques (avions, radio,…) son bon fonctionnement reste essentiellement basé sur l'acteur humain et sur un référentiel de connaissances communes. Pour la gestion des circulations un contrôleur établit pour chaque aéronef qui doit se déplacer, un cheminement et le communique au pilote. Le contrôleur gère donc la simultanéité et la régulation des cheminements, il en assure pour une grande part la sécurité et la performance. La bonne exécution du déplacement est donc conditionnée par une bonne définition de la réglementation et par une bonne application par des opérateurs humains. Les échanges ont lieu sur un canal radio spécifique par un ou plusieurs contrôleurs en fonction de la charge de travail. La conception du système a pour objectif de sécurité d'éviter les situations de collision ou de quasi collision et comme objectif de performance de faciliter les mouvements d'un maximum d'appareils dans un minimum de temps ou d'espace.

Une démarche analytique nous conduit à identifier un espace aérien (la CTR), l'espace de l'avion et à définir des interfaces (radio, règles de circulation,…). Nous considérons les objets génériques suivants :

- Les pilotes, les contrôleurs
- les avions,
- la tour de contrôle,
- l'aérodrome,
- les règles de circulation

L'analyse du système se concentre sur les relations entre les éléments assurant le lien entre les avions et l'espace aérien, à savoir la radio ou les règles. Une démarche analytique doit donc s'attacher à identifier les relations comme autant de flux reliant les organes. Le tableau ci-dessous propose une analyse de ces relations pour la CTR.

de / vers	pilote	avion	contrôleur	tour de contrôle	aérodrome	Règles de Circulation aérienne
pilote	double association (collaboration entre pilote-copilote) (communique avec)	permission (est piloté par)	association (communique avec)			
avion	association (pilote)	double association (évoluent sur le même aérodrome) et (communique avec)	association (contrôle les mouvements de)	association (communique avec)		
contrôleur	association (communique avec)	association (est contrôlé par)	association (collaboration dans la tour)	association (est opérée par)		
tour de contrôle	association (communique avec)	association (est contrôlé par)	association (opère les équipements de la tour)	abstraction (à la fois objet, et système)	association (contient)	
aérodrome	utilisation (fait évoluer son avion sur)	permission (évolue sur)	utilisation (contrôle le trafic sur)	permission (contrôle les mouvements sur)	abstraction (à la fois objet et système)	
Règles de circulation aérienne	utilisation (pilote suivant)	utilisation (évolue suivant)	utilisation (contrôle suivant)	utilisation (contrôle le trafic suivant)	utilisation (impose des mouvements fonction de)	

On constate qu'on retrouve l'essentiel des espaces systèmes associés aux éléments identifiés, et, que des espaces supplémentaires comme un ou des espaces de communication ou un espace d'évolution sont apparus. On distribue ces espaces identifiés en espaces opérants, espaces de décision ou espaces d'information ce qui aboutit un système général comme celui représenté ci-dessous :

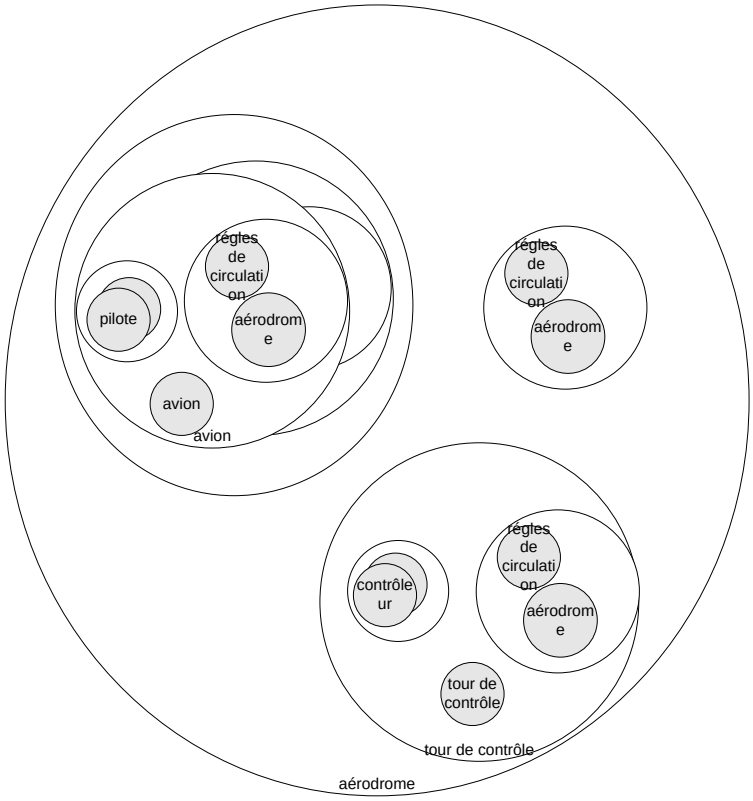


Figure 41 : mauvaise utilisation du modèle de système général

Même si nous avons défini les trois éléments du modèle OID, nous ne démontrons pas l'isomorphisme attendu entre le modèle de système général et le modèle produit. La démarche est passée par la recherche des éléments qui permettent d'identifier les espaces possibles produits à partir de l'espace général et enfin par l'identification des différents constructeurs qui produisent ces sous espaces. En fait, nous avons mené une approche objet. Chaque sous système décision, opérant et information présente une structure différente liée à la nature des objets modélisés. Il est impossible alors de garantir l'isomorphie entre le modèle conceptuel décrit et le modèle de représentation qui va être produit. Cette démarche intuitive fondée sur la connaissance du système global et sur une tentative de représentation des entités identifiées et de leurs relations à partir du modèle de système général ne respecte pas le principe définit par Le Moigne.

Alors, comment utiliser le modèle général simplement et correctement?

En partant du système général lui-même, construire un modèle isomorphe au système général représentant le système gestion des mouvements d'un aérodrome :

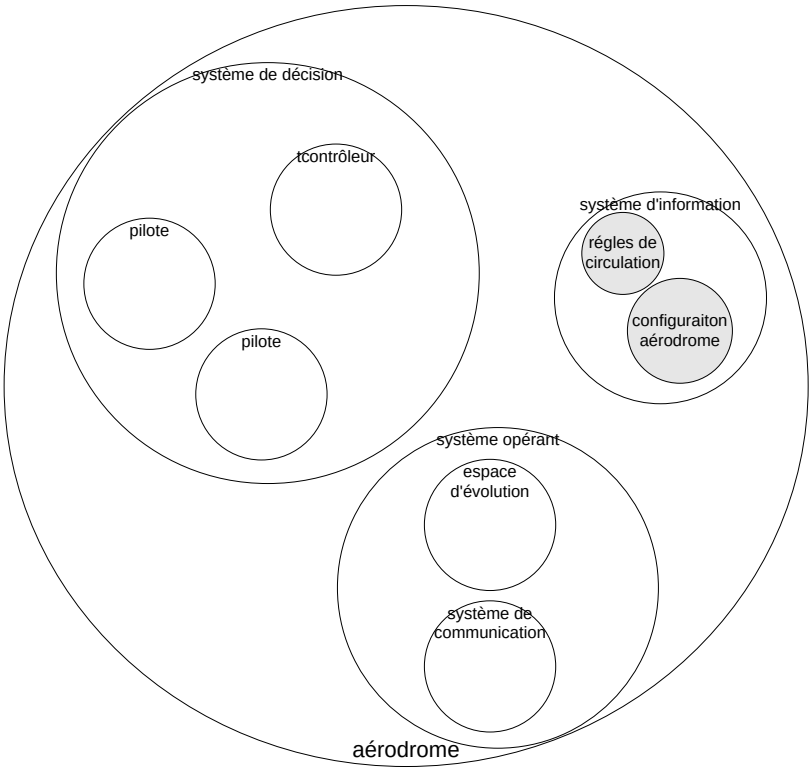


Figure 42 : Système général d'une régulation d'aérodrome

Comme dans toute démarche descendante nous somme partis des éléments identifiés de manière évidente : c'est-à-dire les entités et la connaissance que nous avons de leurs comportements respectifs. Dans les analyses qui ont précédé nous avons postulé que le monde observé est le résultat de la collaboration des trois types de systèmes distincts : l'aérodrome lui-même, la tour de contrôle et les avions. Les systèmes tour de contrôle et avion sont des systèmes organisés dont le comportement est le résultat de l'activité coordonnée des contrôleurs et des pilotes. Ces entités représentent des systèmes actifs qui produisent les espaces correspondants :

- le point de vue de chaque contrôleur pour qui l'espace est composé d'éléments statiques, la configuration de l'aérodrome et les référentiels de connaissances, et, d'éléments dynamiques, les aéronefs.
- Le point de vue de chaque pilote pour qui l'espace est composé d'éléments statiques les référentiels de connaissance et d'éléments dynamiques la tour de contrôle et les autres aéronefs.
- L'avion dans lequel collaborent des pilotes et donc le comportement est le résultat de cette collaboration,
- La tour de contrôle dans laquelle collaborent les contrôleurs pour réguler le trafic.

Chaque point de vue produit construit un espace image de l'espace général dont les propriétés vont être modifiées par un processus de perception et/ou d'acquisition associé au système.

Ce diagramme offre une représentation suffisante du système de gestion des mouvements de l'aérodrome, et permet de différencier les différentes composantes décisionnelles (c'est-à-dire dont la décision modifie les propriétés de l'aérodrome), opérationnels (c'est-à-dire les objets

utilisés pour achever le projet d'action de réguler) et d'information. Il ne préjuge pas de l'organisation des objets en particulier de l'espace de communication.

La différence entre les deux représentations provient essentiellement de la façon dont a été abordé le problème. Dans la première démarche, le problème a été considéré sous son aspect physique, au sens de la chose existante; l'analyse a donc naturellement induit une représentation des objets puis des relations à travers la structure de cette chose observée. La seconde démarche a pas été moins intuitive car abordée par application du modèle OID. L'utilisation de ce modèle ne modifie en rien le principe de modélisation à partir des propriétés du système, il en propose simplement une répartition suivant leur compréhension, cette seconde démarche est celle qu'il faut appliquer.

CONCLUSION

Nous avons dans ce chapitre emprunté à J.L. Le Moigne sa vision d'un système à travers une modèle de système général fondé sur la décomposition d'un système quelconque comme la collaboration d'un système opérant, d'un système de connaissance et d'un système décisionnel. Nous avons montré comment le modèle général OID pouvait être utilisé dans une approche espaces-processus et en particulier comment l'organisation des différents acteurs du comportement du système se traduisait dans les relations intervenant au niveau des propriétés elles-mêmes ou au niveau de leur représentation sémantique.

Ce modèle de système général offre d'un côté une décomposition type suffisante des entités intervenantes dans l'action et d'un autre côté la possibilité d'identifier un tissu relationnel traduisant l'organisation ou l'architecture du système observé. En effet, une approche identificatrice simplifiée des propriétés mise en jeu fournit une vue plus globale des éléments qui composent un système et permettent d'appréhender le comportement collectif de ses parties. Elle permet de progresser dans la modélisation à différents niveaux d'abstraction et de descendre du plus général au plus particulier sans perdre de vue l'organisation de l'ensemble. Chaque propriété étant la perception que l'on peut avoir d'un objet du monde observé. Les relations qui relient les entités vont déterminer et borner des sous espaces sur lesquels il sera possible de conduire une première identification des comportements possible ou de vérifier les comportements attendus. La connaissance des propriétés des relations qui caractérisent ces sous espaces permettra ensuite de déterminer les caractéristiques de la dynamique de chacun. D'un point de vue pratique, l'identification d'entités actives, de systèmes ou de sous systèmes, implique nécessairement que celles-ci incluent un système de décision, un système d'information et un système opérant, et, que l'ensemble des flux (échanges, communications, etc) s'effectuent à travers les relations.

EVALUATION DES RISQUES

INTRODUCTION

Les fondamentaux du modèle étant définis, il reste nécessaire de montrer que ceux-ci sont adaptés à l'ingénierie du risque. Nous montrerons dans un premier temps comment l'approche modélisatrice proposée vient en complément des méthodes analytiques soit pour la simulation et le suivi du comportement du système, soit lors de la mise en collaboration d'experts. Enfin, nous montrerons comment le modèle de représentation proposé peut être transférer sur un espace probabilisé autorisant ainsi la quantification des probabilités d'occurrence de situations ou de chemins de comportements.

IDENTIFICATION DES DIFFERENTES SITUATIONS

De l'approche systémique à l'analyse systématique

En décrivant le feu à travers la relation de dépendance de deux propriétés forme et fonctionnement, nous avons choisi de représenter l'objet perçu, c'est la raison pour laquelle elle nous impose de représenter le feu comme un tout et non comme une simple association de signaux. C'est le fondement de l'approche systémique; ici le feu est perçu et abordé par le message qu'il nous transmet à travers ses différents états.

Cette démarche correspond à une approche naturelle que nous avons d'un système quelconque. En effet, l'approche systémique se définit par rapport à un projet.

Si nous reprenons le carrefour pour lequel nous avons défini une expression de comportement :

$$\text{Carrefour}(X)= (\text{eteint.eteint} + \text{clignotant.clignotant} + (\text{vert}.X^{j} + \text{jaune}.X^{j+1} + \text{rouge}.X^{j+2}).\text{rouge}.X^{m+2} + (\text{vert}.X^{m} + \text{jaune}.X^{m+1} + \text{rouge}.X^{m+2}).\text{rouge}.X^{j+2}).X^{k=2j=2m}$$

Ainsi que nous l'avons déjà vu, cette expression représente l'instanciation d'un espace unique sur lequel nous définissons deux groupes de cinq valeurs de signaux.

Nous pouvons alors mener une démarche analytique de différenciation (par l'observation du graphe équivalent par exemple) pour obtenir les expressions de comportement de chaque groupe de signaux et en déterminer enfin les différentes situations à partir d'une simple association de ces deux groupes.

Nous avons alors mené une démarche analytique systématique d'identification des situations potentielles du système.

De même il est possible d'écrire le comportement du carrefour en définissant un état défaillance représentant l'espace complémentaire des combinaisons de signaux non admis en fonctionnement :

$$\text{Carrefour}(X)= (\text{défaillant} + \text{eteint.eteint} + \text{clignotant.clignotant} + (\text{vert}X^{j} + \text{jaune}X^{j+1} + \text{rouge}X^{j+2}).\text{rouge}X^{m+2} + (\text{vert}X^{m} + \text{jaune}X^{m+1} + \text{rouge}X^{m+2}).\text{rouge}X^{j+2}).X^{k=2j=2m}$$

Néanmoins, cette expression ne correspond pas à la perception du feu par l'usager; toute défaillance du feu conduisant à un état éteint ou clignotant.

Mais, un des points intéressant de la démarche proposée est que l'expression de comportement qui n'est qu'une vision partielle de l'espace de comportement nous permet de générer immédiatement une expression complète de cet espace à travers l'expression :

$$\text{Carrefour}^{*}(X) = (\text{eteint} + \text{clignotant} + \text{vert} + \text{jaune} + \text{rouge})^{*}. X$$

Dans un traitement automatisé des expressions il suffit de remplacer la forme Carrefour(X) par Carrefour*(X) pour traiter l'espace de comportement complet du feu.

De l'approche analytique au projet systémique

La démarche analytique qui a conduit à l'association de signaux a le mérite de nous présenter une espace plus large, et surtout une vision systématique des différents états possibles du feu. C'est aussi l'intérêt du modèle de représentation proposé car à partir d'une expression issue de l'observation ou de la compréhension intuitive d'un comportement, il devient facile d'identifier les composantes et d'en déterminer la combinaison d'états possibles. Cette démarche correspond exactement à l'approche que nous avons suivie dans le chapitre précédent pour aborder les relations de dépendance et leur expression par une relation sur les instanciations des espaces mis en relation dans l'expression :

Forme(X).Couleur(X) = vertical.X^{j}.vert.X^{m} + vertical.X^{j}.jaune.X^{m+1} + disque.X^{j+1}.vert.X^{m} + **vertical.X^{j}.rouge.X^{m+2}** + disque.X^{j+1}.yellow.X^{m+1} + **disque.X^{j+1}.rouge.X^{m+2}** + **horizontal.X^{j+2}.vert.X^{m}** + **horizontal.X^{j+2}.jaune.X^{m+1}** + **horizontal.X^{j+2}.rouge.X^{m+2}**

Nous avons identifié le projet en écrivant en gras les états qui correspondent au comportement souhaité du carrefour. Nous avons ensuite précisé l'objectif en décrivant la relation qui unit *j* et *m*.

Nous venons donc à travers l'approche des relations de montrer l'intérêt que représente le modèle de représentation dans l'analyse et la reconnaissance des situations. Tout objet perçu et présenté à partir d'une approche systémique sera facilement complémenté en déterminant l'espace associatif des propriétés perçues sans avoir à mener une approche analytique.

L'analyse par l'observation ou le retour d'expérience

Dans l'exemple du carrefour routier nous avons considéré un espace de décision en partant d'un monde idéal dans lequel chaque conducteur appliquait les règles du code de la route, l'espace décrit étant celui de la décision attendue. La particularité des systèmes à composante humaine étant la forte individualité et la forte créativité des comportements, on peut légitimement douter que cet espace corresponde à une réalité observable. Cependant, ceci ne remet pas en cause le modèle du carrefour et c'est là un des principaux intérêts de l'approche proposée.
Reprenons l'expression de la décision des conducteurs sur un carrefour

(eteint.(stopper + passer). eteint.((stopper + passer) +

(clignotant.(stopper + passer). clignotant.((stopper + passer)

(vert.passer.X^{j} + jaune.(stopper + passer).X^{j+1}+ rouge.stopper.X^{j+2}).rouge.stopper.X^{m+2} +

(vert.passer.X^{m} + jaune.(stopper + passer).X^{m+1}+ rouge.stopper.X^{m+2}).rouge.stopper.X^{j+2}).X^{k}

Dans le chapitre précédent nous avons considéré l'espace de décision du carrefour en partant d'un monde idéal dans lequel chaque conducteur appliquait les règles du code de la route. En fait l'espace de décision décrit est celui de la décision attendue or la particularité des systèmes à composante humaine est la forte individualité et la forte créativité des comportements. Ceci traduit le fait que pour certaines phases du fonctionnement du carrefour le comportement des véhicules ne peut plus être considéré systématique mais s'individualise fortement. On observe cette individualisation pendant :

- les phases de transition, c'est-à-dire les phases de jaune, voire de début de rouge dans certaines villes ou certains pays,
- les phases où la consigne est moins impérative comme le jaune clignotant, ou chacun franchi le carrefour suivant son interprétation ou sa connaissance du code de la route.

Intéressons nous à la phase de fonctionnement normal d'un feu routier, sous sa forme sémantique :

$$\text{"passer"}.X^{j} + \text{"stopper si possible"}.X^{j+1} + \text{"stopper"}.X^{j+2}$$

Cette expression correspond au comportement souhaité d'un conducteur en présence d'un feu.

Pour la phase "stopper si possible", l'expérience a permis de déterminer un temps de jaune suffisamment long pour permettre à un conducteur de percevoir le changement, d'évaluer sa distance d'arrêt et de stopper si cette distance est suffisante; mais le temps de jaune est aussi suffisamment court pour éviter que les conducteurs ne considèrent cette phase comme une phase de vert. Or, il suffit de se placer à un carrefour dans certaines villes pour constater que les conducteurs ont certaines habitudes de franchissement du jaune, voire du début de rouge, sans que ceci se conclue par une collision. C'est à dire que l'expression du comportement de la propriété décision s'enrichie d'une situation supplémentaire et devient :

(eteint.(stopper + passer).eteint.((stopper + passer) +

(clignotant.(stopper + passer). clignotant.((stopper + passer)

(vert.passer.X^{j} + jaune.(stopper+passer). X^{j+1} + rouge.(stopper+passer).X^{j+2}).rouge.stopper.X^{m+2} +

(vert.passer.X^{m} + jaune.(stopper+passer).X^{m+1}+ rouge.(stopper+passer).X^{m+2}).rouge.stopper.X^{j+2}).X^{k}

Remarquons que dans une approche purement espaces nous sommes obligé de considérer le carrefour dans son ensemble. Si nous passons en approche espaces - processus, nous avons alors pour un même espace général du carrefour des espaces instanciés dont certains offrent un comportement déterminé (l'espace du feu lui-même) et d'autres un comportement moins déterminé (l'espace de décision associé à la perception du feu). Pour les instances d'espaces X^{j+2} et X^{m+2} il est nécessaire d'enrichir l'expression de décision avec des propriétés caractérisant des éléments de décision complémentaires. En fait on peut constater que la décision individuelle est soumise à une évaluation intuitive du risque de collision, et que cette évaluation est le résultat de la connaissance individuelle du carrefour :

- connaissance de la signification des signaux,
- connaissance du fonctionnement général des signaux d'un carrefour,
- connaissance du fonctionnement local du carrefour,
- connaissance du comportement global et local des autres conducteurs,
- contexte du carrefour ou de la circulation générale : les seuils d'appréciation évoluent en fonction de différents critères comme l'encombrement du carrefour ou le temps d'attente au rouge.

Par exemple, l'analyse et l'observation d'un carrefour montrent que les conducteurs ont intégré que le phasage des feux comprend une phase de rouge intégral conséquente leur permettant de franchir le carrefour dans une relative sécurité pendant encore quelques secondes. L'écriture de l'expression de la décision correspondante serait alors :

(eteint.(stopper + passer).eteint.((stopper + passer) +

(clignotant.(stopper + passer).clignotant.((stopper + passer)

(vert.passer.X^{j} + jaune.(stopper + passer).X^{j+1} + rouge.(stopper+passer).X^{j+2} + rouge.stopper.X^{j+3}).rouge.stopper.X^{m+2} +

(vert.passer.X^{m}+ jaune.(stopper + passer).X^{m+1}+ rouge.(stopper+ passer).X^{m+2} + rouge.stopper.X^{m+3}).rouge.stopperX^{m+3}).X^{k}

L'analyse critique, ou "l'avis d'expert"

Le premier objectif d'un modèle de représentation est de fournir une vision synthétique du système ou du phénomène observé permettant une discussion avec une personne compétente sur le domaine précis. C'est ce qu'on appelle l'avis d'expert. La première opération qu'effectue un expert va être de vérifier la prise en compte de point particuliers n'apparaissant pas clairement dans la description du système et ensuite d'analyser le modèle pour détecter des situations amenant des comportements particuliers. Reprenons le pendant de l'expression de comportement du carrefour dans l'espace de connaissances:

("autre régime"."autre régime"+ "autre régime"."autre régime" +

(("passer".X^{j}+"stopper si possible".X^{j+1}+"stopper".X^{j+2})."stopper".X^{m+2} +

("passer".X^{m}+."stopper si possible".X^{m+1}+"stopper".X^{m+2})."stopper".X^{j+2}).X^{k}

Nota Bene : le doublement de l'expression "autre régime"."autre régime" est laissé pour conserver la correspondance avec les régimes transitoires éteint et clignotant.

On constate aisément que lorsque le carrefour est à l'arrêt ou au clignotant, les conducteurs sont soumis à un régime cohérent. Mais écrivons maintenant cette expression pour un feu R11j, c'est-à-dire dont le signal vert est remplacé par un signal jaune clignotant. Celle-ci est alors la suivante :

("autre régime"."autre régime"+ "autre régime"."autre régime" +

(("passer".X^{j}+"stopper si possible".X^{j+1}+"stopper".X^{j+2})."stopper".X^{m+2} +

("autre régime".X^{m}+."stopper si possible".X^{m+1}+"stopper".X^{m+2})."stopper".X^{j+2}).X^{k}

On s'aperçoit qu'une des voies est soumise à un régime différent de celui du carrefour contrôlé. En toute rigueur le conducteur percevant le signal jaune clignotant devra être vigilant à la présence d'un panneau ou aux véhicules débouchant sur sa droite; mais si cette situation peut paraître acceptable un complément d'analyse montrera par exemple que la visibilité est insuffisante, que le comportement des conducteurs n'est pas ou n'est plus celui attendu, etc. Si seul l'avis de l'expert peut apporter une réponse, l'intérêt est que le modèle met en évidence de telles situations qui sans correspondre à une défaillance, représente un risque potentiel.

L'analyse par schéma de processus

Dans les deux paragraphes précédents nous avons considéré l'analyse d'expressions de comportement attendus. Or, nous avons vu que ces propriétés étaient l'expression de relations de dépendance. Ceci implique que le domaine du possible pour les comportements s'exprime sur des espaces résultant de l'association de ces propriétés. Si pour certains modèles moins complexes il peut être suffisant de conduire une analyse systématique des différents cas, certains systèmes complexes peuvent requérir des méthodes d'analyse plus "empiriques" comme la recherche ou la surveillance d'occurrence de schémas de processus particuliers. Ces schémas s'écrivent alors comme des situations ou des expressions particulières.

Cette utilisation des expressions de comportement répond plus à la recherche de processus particulier dans des espaces complexes, mais peu aussi servir dans l'instrumentation d'un système pour reconnaître l'apparition ou l'occurrence de comportements. Par exemple si nous reprenons le carrefour, la décision normale des conducteurs doit conduire à pouvoir instrumenter le carrefour et constater le comportement permanent suivant :

$(vert.passer.X^{j} + jaune.(stopper + passer).X^{j+1} + rouge.stopper.X^{j+2}).rouge.stopper.X^{m+2} +$

$(vert.passer.X^{m} + jaune.(stopper + passer).X^{m+1} + rouge.stopper.X^{m+2}).rouge.stopper.X^{j+2}).X^{k}$

Dans ce cas il faut détecter les franchissements de rouge en différenciant les franchissements francs, c'est-à-dire les situations $vert.passer.X^{m}.passer.rouge.X^{j}$ des franchissements dus à l'utilisation aux limites de la phase de jaunes caractérisées par l'expression :
$(vert.passer.X^{m} + jaune.(stopper + passer).X^{m+1} + rouge.(stopper+passer).X^{m+2}).rouge.stopper.X^{m+2}$
qui apparait immédiatement dans l'expression de comportement.

EVALUATION DU CRITERE D'OCCURRENCE

Transfert sur un espace probabilisé

Nous avons déterminé dans les chapitres précédents qu'il est possible de définir un système à partir de propriétés et d'expressions de comportement. Cette connaissance du système fournit une description des enchaînements d'états relativement aux propriétés de l'objet. Cette démarche doit donc aussi permettre la quantification des critères d'occurrence. Deux approches s'offrent à nous :

- une approche partant de la connaissance de l'occurrence de chaque état
- une approche partant de la connaissance du comportement du système c'est-à-dire de l'occurrence de la transition.

Avant de développer l'une ou l'autre de ces approches il est nécessaire d'opérer un transfert de l'espace objet décrit vers un espace de probabilité.

Soit $p[P, \mathcal{I}]$ une propriété , P est l'espace des réalisations de $p[P, \mathcal{I}]$.

P étant défini par les expressions de comportement, chaque instance p_n d'un objet peut être définie par au moins une suite ordonnée de réalisation $(p_0,\ldots p_n)$ correspondant à une expression, chaque expression P(X) définit donc une partition de P.

On défini Θ la classe des suites de P définies par P(X) expressions de comportement de p[P, $\mathcal{I}$] tels que $P(X) = \sum_{i=0}^{i=n} p_i X^i$; c'est à dire que chaque partie de Θ définit les suites de réalisations conduisant à une instance p_n; le complémentaire de chacune des parties étant l'ensemble des suites de réalisation ne conduisant pas à p_n.

Il apparaît de façon naturelle que (P, Θ) est un espace probabilisable.

Sur l'espace d'instances d'un objet, les différentes instances $p_n X^n$ définissent une suite particulière de Θ des n événements caractéristique de l'occurrence de l'événement (ou situation) défini par P(X) depuis l'instance p_0.

Or d'après la définition de l'instanciation les $p_n X^n$ sont deux à deux incompatibles (sinon il n'y a pas instanciation), il est alors possible de définir une mesure de probabilité pour un objet d'être dans un état qui satisfait aux axiomes :

- $0 \leq \prod(p_n X^n) \leq 1$ pour toute expression comportementale P(X) de p[P, $\mathcal{I}$],
- $\prod(P) = 1$,
- Pour tout suite de $p_n X^n$, alors $\Pi\left(\sum_1^\infty p_n X^n\right) = \sum_1^\infty \Pi(p_n X^n)$

Nous avons opéré un transfert isomorphique de l'espace d'instanciations d'un objet vers un espace de probabilité. L'intérêt de cette démarche est qu'elle permet de conserver les méthodes et outils de d'évaluation probabiliste et statistiques déjà utilisés en Maîtrise de Risques. Par exemple, si nous reprenons l'exemple du carrefour routier pour lequel nous avons établit un modèle de représentation du fonctionnement, nous pouvons alors déterminer un espace de probabilité sur l'espace opérant. Sachant que l'espace d'un feu est défini par la totalité des états des propriétés qui le composent, il est inintéressant de connaître la probabilité d'occurrence de chaque état anormal. Par contre, nous pouvons considérer la probabilité globale de défaillance et la probabilité de fonctionnement normal, cette dernière étant alors la probabilité d'être dans un des états normal de fonctionnement du feu, à savoir : éteint, jaune clignotant, jaune fixe, rouge ou vert.

C'est-à-dire que l'expression défini un espace de réalisation, dit de fonctionnement normal du feu, qui est lui-même un espace de probabilité.

La connaissance des probabilités d'événements par des méthodes formelles de calculs, de mesures ou de statistiques, le modèle proposé rejoint le domaine de l'ingénierie du risque. L'approche fournit simplement des estimateurs fiables sur un comportement avec un minimum d'éléments descriptif du système observé.

Par exemple, dans le cas du carrefour l'étude peut se concentrer sur le fonctionnement cyclique du feu sans remettre en cause les calculs. Reprenons l'expression du carrefour telle que nous l'avions établie au chapitre 0:

Carrefour(X)= (defaillant + eteint.eteint + clignotant.clignotant +
$(vert X^j + jaune X^{j+1} + rouge X^{j+2}).rouge X^{m+2} + (vert X^m + .jaune X^{m+1} + rouge X^{m+2}).rouge X^{j+2}) X^k$

La variable X^k signifie que nous avons un espace commun du carrefour, et chaque variable X^j et X^m représentant le sous-espace de chaque axe de circulation.

Si nous voulons nous intéresser au fonctionnement du carrefour, il est alors possible de traiter séparément les sous espaces X^k, X^j et X^m ; par exemple, à partir de la connaissance des temps de cycles il devient facile de déterminer l'espace de probabilité des états du carrefour sans avoir à se préoccuper des unités et dimensions retenues pour l'expression des valeurs:

état	expression	valeur sur X^i	probabilité sur X
1 - ∏(Fonctionnement(X))	$\lambda = 1,5\ 10^{-7}$	$1,5\ 10^{-7}$	$1,5\ 10^{-7}$
éteint	2 heures par an pour maintenance	$22,831\ 10^{-5}$	$22,831\ 10^{-5}$
clignotant	statistiquement ¼ h par jour	0,0104525	0,0104525
cyclique	le reste du temps	0,98931904	0,98931904

Sachant que l'espace de réalisation complet du carrefour comprend l'ensemble des états, on a ∏ (Carrefour(X)) = 1.

On retrouve bien l'expression du taux de défaillance λ = 1 - ∏ (Fonctionnement(X)).

Chaque expression $vertX^j+jauneX^{j+1}+rougeX^{j+2}$ et $vertX^m+.jauneX^{m+1}+rougeX^{m+2}$ décrit un sous espace de probabilité qui peut se caractériser par la probabilité d'avoir un signal allumé avec

$\prod (vertX^j+jauneX^{j+1}+rougeX^{j+2}) = \prod (vertX^m+.jauneX^{m+1}+rougeX^{m+2}) = 1$

Nous retrouvons ainsi, les méthodes d'estimation des arbres de défaillances. Le couplage entre les expressions de comportement et la notion d'espace de probabilité présente un intérêt dans des démarches plus complexes. De même, le couplage entre les expressions de comportement et l'espace de probabilité permet d'aborder les problèmes de dépendance d'état en fonction de la nature des propriétés :

- Les probabilités d'états sont indépendantes entre elles mais dépendantes des probabilités de transition,
- Les probabilités d'états sont toutes dépendantes.

<u>Probabilités d'états dépendantes des probabilités de transitions</u> :

Si chaque réalisation de l'objet $p[P,\mathscr{T}]$ est indépendante, on déduit que sur l'espace probabilisable (P, Θ), chaque p_n peut être assimilé à un événement dont la probabilité d'occurrence est déterminée par deux événements indépendants : la probabilité de l'événement précédent et la probabilité de transition entre les deux instanciations. Le processus est entièrement déterminé par les conditions initiales (probabilité de l'instance initiale) et les probabilités de transitions. C'est-à-dire que la loi de probabilité sur l'espace (P, Θ) est une chaîne de Markov

La probabilité de transition entre deux instances de $p[P,\mathscr{T}]$ peut être définie par l'égalité de Chapman – Kolmogorov : $\Pi_{0,n}(p_0, p_n) = \sum \Pi_{0,k}(p_0, p_k) \cdot \Pi_{k,n}(p_k, p_n)$ qui présuppose la connaissance de la chaîne, c'est-à-dire des p_k.

Chaque instance p_n étant le résultat d'une expression $P_n(X) = \sum_{i=0}^{i=n} \sum_{j=0}^{j=card(O)} \delta_{i,j}\, p_i X^i$ qui décrit la trace des transitions sur P.

La probabilité d'occurrence d'une instance p_n sera alors donnée par l'équation : $\Pi_{0,n}(p_0, p_n) = \sum_{i=1}^{i=n} \sum_{j=0}^{j=card(O)} \delta_{i,j} \Pi_{i,i+1}(p_i, p_{i+1})$

La matrice d'instanciation pondérée des probabilités de transition devient alors la matrice de transition de la chaîne.

Probabilités d'états dépendantes :

La probabilité d'instance d'une propriété est dépendante de la probabilité des instances précédentes. Si chaque réalisation de l'objet p[P,Ṗ] est dépendante, on déduit que sur l'espace probabilisable (P, Θ), chaque p_n peut être assimilé à un événement dont la probabilité d'occurrence est déterminée par $\Pi(p_n) = \Pi(p_0) \cdot \prod_{i=1}^{i=n} \Pi(p_i | p_{i-1}, ..., p_0)$, $p_{i-1}, \ldots, p_0$ appartenant à la suite définie par l'expression de comportement $P_n(X) = \sum_{i=0}^{i=n} p_i X^i$.

En ne s'intéressant qu'à l'expression de comportement on remarque que dans le cas particulier d'événements dépendants d'une propriété, les instances de l'objet et les transitions définissent un graphe causal <{pi}, $\left\{\frac{dp_i}{di}\right\}$>.

Ce graphe associé à l'espace probabilisé (P, Θ, ∏) permet de déterminer les probabilités de chaque nœud (instance) telles que :

$$\Pi(p_{1,\ldots,} p_n) = \prod_{i=1}^{i=n} \Pi\left(p_i \left| \left\langle < \pi_{i-1}, \left\{\frac{dp_{i-1}}{di}\right\} \right\rangle \right.\right).$$

L'opération revient à calculer la probabilité de chaque nœud (instance) d'un graphe en propageant les probabilités conditionnelles d'instances liés les unes aux autres par un réseau de cause à effets. Nous avons là la définition d'un réseau bayésien qui est le résultat d'un graphe causal et d'une représentation probabiliste.

CONCLUSION

Nous avons brièvement abordé dans ce chapitre l'utilisation de l'approche modélisatrice *espaces – processus* dans une démarche d'analyse des risques. Néanmoins, nous avons montré comment le fort couplage au langage par les unités sémantiques permet de conduire des analyses d'expert sur le modèle. En particulier, l'indépendance du modèle de représentation vis-à-vis de la structure du système permet une utilisation du modèle tout au long de la vie de ce système nonobstant les modifications structurelles qu'il peut subir.

Enfin, le transfert de l'espace du modèle vers un espace probabilisé permet d'utiliser les outils formels de quantification des probabilités d'occurrence des situations, et même de conduire des analyses statistiques des comportements.

CONCLUSION ET PERSPECTIVES

SYNTHESE DE L'APPROCHE PROPOSEE

Si comme nous l'avons vu dans la première partie de ce mémoire, les méthodologies de l'ingénierie du risque sont suffisantes pour un système entièrement constitué d'objets techniques. En effet, l'essentiel des événements que subit un système technique est constitué par des défaillances ou une variation de l'environnement qui sont identifiées dès la conception ou surveillées pendant la durée de vie du système. Pour un système complexe, dont les ressorts du comportement ou de l'évolution résultent eux-mêmes de causes complexes, les outils de l'ingénierie du risque ne suffisent plus, il est nécessaire d'appréhender le système à travers des approches systémiques prenant mieux en compte l'impact de l'organisation. Les approches proposées ne permettent pas aujourd'hui une modélisation du système totalement systémique, une nouvelle approche conceptuelle a été proposée.

Le travail présenté dans ce mémoire n'apporte bien sûr pas de réponse scientifique ou technique à ce que seul l'esprit humain peut appréhender, mais propose :

- une représentation naturelle et unifiée de la perception d'un système à partir de la notion de propriétés et de comportements,
- une approche descriptive et modélisatrice purement systémique dans laquelle le système n'est décrit qu'à travers les éléments perçus : ses propriétés et ses comportements.

Cette approche se traduit par un paradigme espaces – processus : ***tout système peut se définir comme un projet d'action, c'est-à-dire comme une combinaison Espaces – Processus, les espaces contenant toutes les conditions et moyens nécessaires à l'achèvement du processus.*** Ce paradigme exprime simplement qu'un système peut être vu à travers le comportement des différentes propriétés des entités intervenantes. Ainsi, nous avons défini un modèle permettant de ne décrire que ce qui est caractéristique de l'action de façon à ne retenir que les concepts pertinents de la chose observée. Pour étudier le mouvement d'un véhicule ne sont considérés que la masse et la vitesse. La couleur et la marque importent peu. Néanmoins, et ce afin que ce modèle ne reste pas qu'une vision conceptuelle de la dynamique d'un système, un modèle de représentation naturel de la propriété et puis de son comportement a été défini. Ce modèle de représentation s'appuie sur les expressions rationnelles qui permettent de décrire à partir du langage courant les expressions de comportement. Néanmoins comme toute description nécessite un minimum de rigueur d'expression et d'organisation, une notation unifiée de la propriété a été proposée : incluant identifiant – au sens du modèle-, domaine de définition et représentation sémantique. Il est ainsi possible d'utiliser indifféremment identifiants ou unité sémantiques pour construire les expressions rationnelles.

Ensuite, afin de pouvoir manipuler ces expressions de façon simple, et surtout de façon à pouvoir déterminer des modèles de calcul, une d'expression de comportement a été proposée sous la forme suivante:

$$P(X) = \sum_{i=0}^{i=t} p_i X^i \ .$$

Il a été montré que cette forme algébrique permet l'utilisation des outils mathématiques permettant d'évaluer et d'analyser un système sous le point de vue de la maîtrise des risques et est compatible d'une vision macroscopique que propose un modèle général systèmes opérants – informations – décisions, dit modèle OID.

Apports méthodologiques et pratiques

L'approche espaces – processus proposée continue à s'inscrire dans ce cadre fondamental de l'ingénierie du risque :

- D'un point de vue purement maîtrise des risques, l'approche intègre le paramètre humain dans le système et en particulier dans l'action résultante. Étant donné que le comportement humain est très étroitement lié à la connaissance qu'il a soit du comportement du système, soit des situations rencontrées, l'approche considère que celle-ci est une composante à part entière du système, et par conséquent du modèle. Enfin, toute nouvelle approche se doit d'offrir une capacité d'évolution du modèle du système au cours de sa vie, et la prise en compte de l'évolution des performances pour ne pas rester à une simple modélisation lors de la conception.
- D'un point de vue modélisation système, l'approche est essentiellement un complément aux approches systémiques, qui aujourd'hui, utilise des modèles de représentation structurels.
- Enfin, à travers l'intégration du facteur humain et des connaissances comme partie intégrantes d'un système, l'approche espère offrir un outil complémentaire aux cindyniques en leur permettant d'identifier et de représenter les propriétés caractérisant les Déficits Systémiques Cindynogènes dans le comportement d'un système.

D'un point de vue pratique l'approche espaces – processus permet d'augmenter considérablement l'utilité d'un modèle ; en dehors du fait de conserver la lisibilité du modèle au-delà du niveau conceptuel, un modèle espaces – processus n'étant ni fonctionnel ni organique celui-ci peut soit, continuer à représenter le système réel quelque soit sa structure physique, soit évoluer avec l'évolution que l'on a de sa perception. Ainsi, un modèle espaces – processus permet d'inscrire la modélisation dans le cycle de vie du système ; le modèle n'a alors pas qu'une simple utilité d'évaluation en vue de modification ou d'analyse de cas, mais continuant à vivre avec le système il s'inscrit complètement dans une démarche de retour d'expérience et de suivi du fonctionnement. Le modèle ne se pose plus alors en simple outil d'analyse mais comme un moyen d'aide à la décision dans le management du système. Ce dernier point est important car il implique que le modèle conserve une certaine indépendance par rapport au système construit; celle-ci se réalisant dans la conceptualisation et la robustesse du modèle de représentation.

Apports conceptuels

Même s'il est possible de déterminer différents apports conceptuels dans la modélisation d'un système, le principal apport de l'approche espaces – processus proposée est de permettre de mener une démarche systémique intégrale. En effet, les différentes approches ou méthodologies abordées dans ce mémoire montrent qu'à un moment donné – en particulier dans la représentation – il est nécessaire de revenir à une approche analytique. En effet, si la démarche systémique présente l'avantage d'une meilleure appréhension de la complexité, elle ne permet pas facilement de montrer la fiabilité ou la confiance dans les résultats du modèle. Pour cette raison, les démarches systémiques sont utilisées comme crible pour isoler les éléments essentiels au projet d'action qui sont ensuite traité sous une forme analytique. Ici fiabilité et confiance dans les résultats reposent sur la propriété d'endomorphisme de l'instanciation. En effet, toute propriété se comportant sur son domaine de définition, la mise en relation de deux propriétés va définir un comportement qu'il est possible de maximiser à partir de la combinatoire des domaines de définition des propriétés.

De même, les démarches systémiques sont des démarches essentiellement conceptuelles utilisant les formes sémantiques pour s'exprimer ; la forme sémantique peut difficilement être conservée dans un modèle de représentation ou un modèle de calcul. C'est pourquoi, il est nécessaire de procéder à une classification des concepts ou une transformation de la représentation. Ici, la forme sémantique, toujours associée à la représentation, permet grâce aux expressions de comportement de ne pas opérer de transformation. Nous limitons alors la distorsion et même à travers la manipulation de la forme algébrique, nous conservons compréhension et sens des concepts identifiés. La forme choisie de représentation est neutre, mais permet en outre de continuer à partager le contenu du modèle avec les différents types d'intervenants quelque soit leur culture, à la simple condition qu'ils partagent le langage. Enfin, la démarche systémique est une démarche entièrement dédiée à l'appréhension de la dynamique des systèmes. Les caractères de cette dynamique apparaissent souvent dans la classification des concepts dégagés. Dans l'approche espace-processus la forme proposée autorise la manipulation des éléments de comportement en conservant la lisibilité des concepts.

Un des éléments le plus difficile à déterminer dans une approche systémique est la décidabilité des résultats. La propriété d'endomorphisme de l'instanciation nous a permis d'utiliser un des modèles généraux de la systémique qui présente la particularité de permettre une modélisation d'un phénomène par une approche qui peut indifféremment être macroscopique et microscopique. Cette modélisation permet surtout une analyse itérative du phénomène sans remettre en question le modèle à chaque tour.

Nous avons donc avec l'approche proposée défini une modélisation intégralement systémique, dans le sens où celle-ci permet de conserver à travers toutes les étapes de construction du modèle la démarche intellectuelle systémique.

Le second apport conceptuel de la démarche espaces – processus réside dans la réduction de la complexité qu'elle propose. En effet, la complexité des systèmes trouve souvent son origine dans la forte composante humaine, en ceci qu'elle représente le principe même du système autonome. En particulier, la composante humaine met en œuvre un raisonnement dont les résultats sont le fruit d'un jugement purement individuel et d'une connaissance acquise. Un des apports essentiels de l'approche proposée est de pouvoir considérer avec une même représentation des éléments aussi différents que des objets technologiques, des comportements humains et du savoir par une représentation unifiée de la description du fonctionnement d'un objet opérant, de la connaissance qu'on en a, et du raisonnement amenant à la décision; chacun étant décrit comme des propriétés comportementales. Ce pont apparaît en particulier dans la prise en compte de l'opérateur humain. Or, il n'est pas toujours possible ou même pertinent dans une conception ou un analyse système de considérer l'individualité. Dans la conception d'un système, l'objet humain est abordé sous son aspect comportement attendu par le système (un rôle) qui est défini par un couple acteur – règles d'utilisation de l'objet technique. L'entité humaine représentée dans le système n'est qu'une association de communications avec les objets techniques du système et les règles de comportement associées. Le rôle s'humanise alors par l'instanciation qui se produit dans un premier temps lors de la formation, puis à chaque prise de poste où l'individu devient actif dans le système. A moins de connaître chaque individualité, un tel raisonnement n'est pas toujours applicable.

Si on revient au modèle de système général, on peut constater que certains espaces regroupent des objets de même type. Il devient alors dans ce cas intéressant de considérer l'espace de décision globalement pour effectuer une démarche statistique : les propriétés n'étant plus décrites par individu mais sous la forme d'une propriété commune dont le comportement obéit à des lois statistiques. Par sa répétition, la structure même du système général définit chaque entité

comme la collaboration d'un système décisionnel, d'un système opérant et d'un système d'information, c'est-à-dire comme un espace incluant des objets décisionnels, informations ou opérants. L'utilisation d'un système général dans la modélisation d'un système offre donc la capacité d'une forme fractale de représentation dont l'élément maximisant est l'espace général incluant tous les objets et toutes les relations observables. La particularité de l'espace général est qu'il est possible d'y identifier des objets dont on ne peut déterminer s'ils sont du type décisionnel, opérant ou information. C'est-à-dire que l'espace général est un espace qui peut être défini vis-à-vis de projet d'action mais sur lequel il est possible d'identifier des systèmes autonomes. Le niveau inférieur de répétition sera déterminé par la présence d'espaces composés d'une d'espaces élémentaires de type unique : décision, opérant ou connaissance.

Admettre la vision d'un système par la vision de projet d'action n'est pas quelque chose de nouveau. En dehors des travaux sur la modélisation systémique qui ont littéralement axé leur approche sur ce paradigme, toute conception ou exploitation d'un système effectue cette démarche intellectuelle. En effet, l'ensemble des méthodes utilisent des processus récursifs basés sur l'expression de spécifications générales agissant comme des objectifs à atteindre; l'ensemble des actions est mis en œuvre pour atteindre cet objectif, et se modifie dans le temps en fonction des retours d'expérience ou de l'augmentation de la connaissance sur le système.

Ainsi l'apport conceptuel essentiel de l'approche espaces – processus est d'intégrer dans le modèle une dimension chronologique complexe permettant l'appréhension de la dynamique des systèmes non pas sous le seul aspect séquentiel ou temporel mais sous formes de comportements et de transformations.

Pour résumer cette vision d'un système a travers le projet d'action, confions la conclusion a Jean de la Fontaine : "En toute chose, il faut considérer la fin".

RECHERCHES COMPLEMENTAIRES

Evaluation des critères de gravité

Un des principaux apports de la démarche espaces – processus et de son formalisme est dans la possibilité de définir des critères de dangerosité dans la description d'un système.

En effet, la dangerosité est évaluée à partir des conséquences potentielles d'une situation donnée. Ces conséquences potentielles sont souvent associées à l'occurrence de critères particuliers qui peuvent être des réalisations de propriétés ou l'association d'instances de propriétés. La connaissance à priori de ces réalisation permet d'identifier rapidement dans le modèle les comportements qui y aboutissent. Il est ainsi possible, de déterminer les conditions d'apparition de la situation, d'en déterminer les précurseurs ou même de déterminer les propriétés sur lesquelles porter les mesures de couverture. Pour avoir une démarche quantifiée, il suffit possible de pondérer les instances et de définir les critères d'occurrences associés de façon à pouvoir établir des filtres.

On a montré dans les chapitres précédents qu'un objet peut être décrit par ses propriétés et le comportement de ses propriétés à travers des expressions polynomiales. On a aussi montré que l'instanciation définissait une dimension permettant de traiter les comportements des propriétés sous une forme algébrique. Cette démarche permet de considérer sur un même objet des espaces de comportement différents; c'est-à-dire que l'appartenance au même espace objet maintient les relations et en particulier leurs conséquences. Il est ainsi possible de construire un nouvel espace d'instanciation à partir de deux espaces d'instanciations différents par l'intermédiaire d'une relation d'association et en particulier de créer des associations pouvant être assimilées à des points de

mesures dont ont peut observer le comportement et qui restent neutres vis-à-vis de la dynamique de l'objet.

En particulier, il est possible de définir un constructeur d'espace de danger par l'association de propriétés de l'espace observé. En pondérant les propriétés de l'espace résultant, il est ainsi possible d'obtenir presque directement une mesure complexe occurrence – gravité.

Le rapport au modèle objet

Le rapport au modèle objet qui apparaît dans les définitions précédentes n'est bien sûr pas fortuit. Le rapport entre les deux modèles conceptuels ne trouve pas uniquement son origine dans le fait que l'approche systémique est une approche entités – relations, et inversement qu'une approche objet est une approche systémique, mais est justifié par trois contraintes importantes :

- la nécessité de proposer une démarche descriptive relativement naturelle,
- la nécessité de pouvoir passer du général au particulier et du particulier au général,
- la nécessité de conserver une relation isomorphe entre les éléments du modèle conceptuel et les éléments des modèles de représentation et de calcul.

D'une manière générale la description d'un espace doit s'attacher à dégager par une démarche d'abstraction, l'organisation, la mise en relation et l'articulation de structures qui définissent un espace qualifié de favorable à l'exécution d'un projet d'action, c'est-à-dire que la modélisation cherche à identifier les éléments caractéristiques d'un comportement. Or l'étude d'un système ne doit pas se contenter d'analyser un comportement donné, mais doit aussi nécessairement prendre en compte l'agencement des parties pour en faire émerger des comportements. L'approche objet repose à la fois sur une démarche systémique, telle que nous l'avons définie, et sur une démarche de décomposition. Ainsi, en approche objet le système est caractérisé par ce qu'il est et par ce qu'il fait. Cette démarche est une démarche arbitraire qui procède de l'identification des caractéristiques communes des objets puis de la description de ces caractéristiques sous la forme d'un domaine de définition d'un ensemble. Ce domaine de définition est défini par des attributs, c'est-à-dire un ensemble de caractéristiques et un ensemble d'opérations décrivant un comportement. Ce domaine de définition définit une classe d'objet. Pour ne pas polluer le raisonnement sur un modèle par ce que le système est, le concept d'objet a été remplacé par le concept d'espace, mais les mécanismes de conceptualisation et de représentation de l'approche espaces – processus resteront les même que ceux d'une approche orientée objet.

De même, nous avons déterminé que les espaces sont construit par des relations de généricité, partage, dépendance, influence, association. Nous retrouvons la représentation de ces relations sous les formes suivantes :

- Les relations d'associations du système qui représentent un couplage entre deux propriétés d'objets différents.
- Les relations de généralisation ou de spécialisation, c'est-à-dire que deux objets (classes ou instances différentes) partageant ou différenciant des propriétés ou des opérations. Ces relations font appel à la nature même de la classe mais représentent des particularités différentes.
- Les relations de dépendance :
  - relation d'abstraction qui relient deux objets (ou classes) différentes qui représentent le même concept mais à des niveaux différents.
  - Liaisons sur les propriétés de la classe,

- Permission : relation autorisant un objet à accéder une propriété d'un autre objet,
- Utilisation : un objet requiert la présence d'un autre objet

Si les relations d'association sont des relations structurelles, en ce sens que l'association même des entités définie un système potentiel, les associations de hiérarchie et de dépendance sont des relations sémantiques, c'est-à-dire sur la nature des propriétés.
De la même façon qu'il y a des classes de relations, il existe des classes de constructeurs qui sont différenciées par les propriétés des relations constructives d'espace, c'est-à-dire qu'il est alors possible de considérer l'espace comme une classe d'objets abstraits qui permet de compléter les définitions précédentes.

Modèle de calcul informatique et modèle de connaissances

Un des intérêts de la modélisation proposée dans l'approche espaces – processus est qu'elle est homomorphe, c'est-à-dire que la chose représentée est l'image de la chose perçue. Les notations et représentations choisies sont très volontairement très proches des concepts objets de l'informatique, ceci afin de conserver cette propriété de la démarche dans la définition d'un modèle de calcul informatique.

Une première recherche complémentaire peut viser à définir le cadre de travail permettant à partir de la saisie d'une observation de construire le modèle associé et offrant toute la panoplie d'outils combinatoires, statistiques et probabilistes permettant d'exploiter le modèle de représentation.

Une seconde étape peut viser à partir de la définition de modèle simple à créer automatiquement des systèmes résultants par la mise en relation.

Mais l'intérêt principal d'un modèle de calcul informatique réside en sa représentation formelle des propriétés qu'il serait ainsi possible de coupler avec une base de connaissance. En effet, l'informatique permet le traitement efficace de grandes quantités de données. Dans les approches analytiques les données sont classifiées et rangées le plus souvent dans des tableaux. Les systèmes relationnels définis n'ayant que pour objectif d'optimiser le rangement et l'exploitation de ces listes de valeurs. Or, les connaissances sont avant tout des représentations humaines de concepts acquises soit par un brut apprentissage soit par la déduction.

Un des avantages de l'approche proposée est de ne pas dénaturer la perception à travers le modèle de représentation, ce qui permet une mémorisation de données quasiment brutes. Mais surtout, le modèle espaces – processus permet la représentation de comportement sous forme de séquences. Certaines séquences peuvent alors devenir caractéristiques de comportements. L'expression de comportement est alors une forme facile à exploiter informatiquement.

Enfin, et pour terminer ce mémoire, l'approche modélisatrice proposée n'est pas uniquement exploitable pour la maîtrise des risques mais peut intervenir partout où il est nécessaire de modéliser des systèmes complexes à forte composante humaine.

Sa capacité à construire un modèle de calcul homomorphe à la réalité perçue capable de s'enrichir sans se remettre en cause offre des débouchés sur tous les domaines de l'aide à la décision industriels, civils ou militaires.

BIBLIOGRAPHIE

Ouvrages et articles

[ANDRE 1996]: SyncCharts: A Visual Representation of Reactive Behaviors – C. ANDRE – rapport de recherche RR 96-56, I3S, Sophia Antipolis, 1996.

[ANDRE 2003] : Semantic of Syncharts, projet SPORTS – C. ANDRE – rapport de recherche RR-2003-24-FR, I3S, Sophia Antipolis, 2003.

[ANDRE 2005] : Comparaison des styles de programmation de langages synchrones, rapport de recherche RR2005-13, I3S, Sophia Antipolis, 2005.

[BELLOT 2002] : Fusion de données avec des réseaux bayésiens pour la modélisation des systèmes dynamiques et son application à la télémédecine – D. BELLOT – Thèse de l'Université Nancy 1 2002.

[BEHM 1996] : Développement formel des logiciels sécuritaires de METEOR - Pierre BEHM, MATRA Transport International - first B Conférence, 1996.

[BERRY 1992] : The Synchronous Programming Language ESTEREL: Design, Semantics, Implementation, Science of Computer Programming - G. BERRY, G. GONTHIER - 1992.

[BERRY 1999] The Constructive Semantics of Pure ESTEREL, Draft 3. - G. Berry - CMA, Ecole des Mines and INRIA, 1999.

[CONRUYT 1994] : Amélioration de la Robustesse des Systèmes d'Aide à la Description, à la Classification et à la Détermination des Objets Biologiques – N. CONRUYT – Thèse de l'Université Paris IX – Dauphine 1994.

[COUREAUNAU 2003] : Mise en œuvre de la nouvelle approche d'analyse des risques dans les installations classées - J.C. COURRONNEAU - 2003.

[DALPONT 2003] : Sécurité et gestion des risques - J.P. DALPONT - Techniques de l'ingénieur SE 12. 2003.

[DAMASIO 1999] : Le sentiment même de soi - A. DAMASIO - Editions Odile Jacob 1999, traduction française de "The feeling of what happens. Body and emotion in the making of conciousness", Harcourt, 1999.

[DAVIS 1993] : What is a Knowledge Representation? - R. DAVIS, H. SHROBE, and P. SZOLOVITS - MIT AI Magazine, 14(1):17-33, 1993

[DESFORGES 1997] : Utilisation de la méthode B pour la conception des logiciels critiques d'automatismes ferroviaires - Pierre DESFORGES - paru dans la revue RATP : Recherche et Développement - faits marquants 1997

[DESFORGES 1996] : L'industrialisation de la méthode B - Pierre Desforges - la lettre B, 1996

[EMS 1998] : European Macrosismic Scale 1998 (EMS-1998) sous la direction de G GRÜNTHAL, Conseil de L'Europe, Cahier du Centre Européen de Géodynamique et Sismologie – Volume 19 – 1998.

[FRANCHINI 1999] : Paradoxes et nouvelles orientations du facteur humain en sûreté de fonctionnement – H FRANCHINI – revue l'ARMEMENT numéro 67, septembre 1999.

[FRANCOIS 1993] : La systémique, un méta-langage connectif – C. FRANCOIS – Revue Internationale de Systémique vol 12, n°4-5, 1998.

[GERNIGON 1998] : Histoire de la signalisation ferroviaire - A. GERNIGON - LA VIE DU RAIL, 1998.

[GROSSER 2002] : Construction itérative de bases de connaissances descriptives et classificatoires avec la plate-forme à objets IKBS – D GROSSER – Thèse de l'Université de la Réunion 2002.

[HANQUIEZ 2003] : Evaluation des risques, les résultats dans un document unique - A. HANQUIEZ – Technique de l'ingénieur SE 3 200. 2003.

[HAREL 1985]: HAREL D. , PNUELI A. On the development of Reactive Systems in Logics and Models of Concurrent Systems. NATO ASI Series, K.R APT Ed. Springer Verlag, vol 13, 1985.

[HAREL 1987]: Statecharts : A visual Approach to Complex Systems, Science of Computer Programming Vol 8-3- D. HAREL - 1987.

[HEYLIGHEN 1999]: The Science of self-organization and adaptivity – F HEYLIGHEN – Free University of Brussels. The encyclopedia of life support systems. 1999.

[INES 2001] : INES, échelle internationale des événements nucléaires, manuel de l'utilisateur – Ed. LAVOISIER – 2001.

[KAFKA 1999] : how safe is safe enough? – An unresolved issue for all technologies, Safety and Reliability, - P. KAFKA -ESREL 99, vol 1.

[KEHREN 2003] : Evaluation qualitative de systèmes physiques pour la sûreté de fonctionnement – C KEHREN et C SEGUIN – ONERA CERT. 2003.

[KERVERN 1991] : L'archipel des dangers – G.Y. KERVERN, P. RUBISE - ECONOMICA, 1991.

[KERVERN 1995] : Eléments fondamentaux des cyndiniques - G.Y. KERVERN – ECONOMICA, 1995.

[KERVERN 1999] : Cyndiniques les pistes d'une formalisation – G.Y. KERVERN – Ecole d'été "Gestion Scientifique du risque " septembre 1999.

[KULHMANN 1986] : Introduction to Safety Science, Spriunger – Verlag - A. KULHMANN - New York 1986.

[LANNOY 2003] : Retour d'expérience technique - A LANNOY - Techniques de l'ingénieur SE 1 041. 2003

[LESBATS 1999] : Contribution à l'élaboration d'une science du danger - : M. LESBATS, J. Dos SANTOS, P. PERILHON - Ecole d'été "Gestion Scientifique du risque " septembre 1999.

[LE MOIGNE 1990] : La modélisation des systèmes complexes - J.L. LE MOIGNE - DUNOD, 1990.

[LE MOIGNE 1977] : Théorie du système général : théorie de la modélisation - J.L LE MOIGNE - PUF 1994 (dernière édition).

[LIEVENS 1976] : Sécurité des systèmes - C. LIEVENS - CEPADUES,1976

[LIGERON 1974] : Utilisation des techniques de fiabilité en mécanique - J.C. LIGERON, C. MARCOVICI - Technique et documentation, 1974.

[MEINADIER 2004] : Interrogation sur la complexité des systèmes et la maîtrise de leur technologie et donc de leur ingénierie – J.P. MEINADIER – séminaire Ingénierie de Systèmes, Polytechnique, 2004.

[MILLOT 1999] : Systèmes homme-machine et automatique – P. MILLOT – Journées doctorales d'automatique, septembre 1999.

[MORIN 2002] : A propos de la complexité - E MORIN - intervention au CNRS 2002.

[MORTUREUX 2004] : Le retour d'expérience en question - Y MORTUREUX - Techniques de l'ingénieur SE 1 040. 2004.

[NORSYS 1997] : NETICA Application for belief networks and influence diagrams – NORSYS Software Corp. 1997.

[NAIM 2004] : Réseaux bayésiens – P. NAIM, P.H. WUILLEMIN, P. LERAY, O. POURRET, A. BECKER – EYROLLES, 2004

[NICOLET 1999] : De l'erreur humaine à la défaillance systémique – J.L NICOLET – Ecole d'été "Gestion Scientifique du risque " septembre 1999.

[PENALVA 1999]Situations et systèmes complexes – J. M. PENALVA - Ecole d'été "Gestion Scientifique du risque " septembre 1999.

[PERILHON 2003] : MOSAR présentation de la Méthode - P PERILHON - Techniques de l'ingénieur SE 4 060, 2003.

[PERILHON 1999] : Réflexion sur les modèles de la science du danger – P. PERILHON - Ecole d'été "Gestion Scientifique du risque " septembre 1999.

[POINT 2000] : AltaRica : Contribution à l'unification des méthodes formelles et de la sûreté de fonctionnement – G. POINT – Thèse de l'Université de Bordeaux I, 2000.

[QUENIART 1996] : Analyses de sûreté, principes et pratiques - D. QUENIART - Techniques de l'ingénieur B 3 810. 1996.

[ROUX 2000] : Langages réactifs synchrones et asynchrones - O. ROUX – Techniques de l'ingénieur Informatique industrielle ISSN 1632-3831. 2000, vol. S3, noS8060.

[SIGNORET 2005] : Analyse des risques des systèmes dynamiques - J.P. SIGNORET - Techniques de l'ingénieur SE 4 070 et SE 4 071. 2005 .

[SHANNON 1948] : A Mathematical Theory of Communication – C.E. SHANNON – The Bell System Technical Journal, october1948

[STARR 1969] : Social baufit versus technological risk. What is our society. Willing to pay for safety ?- C. STARR - Science, vol 165, september 1969.

[VERDEL 2000] : Méthodologies d'évaluation globale des risques – Application potentielles au Génie Civil, T. VERDEL – Ecole des Mines de Nancy. Congrès risques et génie civil. Paris, 2000.

[TANZI 1999] : Modélisation synchrone appliquée à la sûreté de fonctionnement – T.J. TANZI, C. ANDRE

[TANZI 2006] : Ingénierie du risque – T.J. TANZI, F. DELMER – Collection sciences et technologies, Ed Hermès-Lavoisier, 2006.

[VEROT 1999] : Maîtrise du risque, le retour d'expérience - Y. VEROT – Ecole d'été "Gestion Scientifique du risque " septembre 1999.

[VIVALDA 1999] : Modèles simples de comportement humain appliqués au transport maritime – C. VIVALDA - Ecole d'été "Gestion Scientifique du risque " septembre 1999.

Textes réglementaires

[SIST] : Loi n°2002-3 du 03/01/2002, relative à la sécurité des infrastructures et des systèmes de transport, appelée « loi SIST ».

[STPG] : Décret relatif à la sécurité des transports publics guidés, du 03/06/2003, appelé « décret STPG ».

Textes normatifs

[CNET 1993] : CNET , recueil de fiabilité, 1993.

[DEF 1996] : DEF STAN 00-56 : Safety Management Requirements for Defence Systems, part 1 and 2. 1996.

[EN50126] : EN 50126 Applications ferroviaires, spécification et démonstration de la sûreté de fonctionnement, fiabilité disponibilité maintenabilité et sécurité (FDMS). Norme Européenne 1999.

[EN50129] : EN 50129 : Applications ferroviaires, systèmes électroniques relatifs à la sécurité pour la signalisation, 2003.

[EN50155] : EN 50155 Applications Ferroviaires, équipements électroniques utilisés sur du matériel roulant. Norme Européenne, 2002

[EN50128] : ENV 50128 : Applications ferroviaires, systèmes de signalisation, de télécommunication et de traitement – Logiciels pour systèmes de commande et de protection ferroviaire. Norme Européenne, 2001.

[EN50159] : EN50159 : Applications ferroviaires, systèmes de signalisation, de télécommunication et de traitement. Norme Européenne. 2001.

[EN61508] : EN 61508-5 : Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité, 2002.

[IEEE 1984] : IEEE STD 500-1984 : Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear-Power Generating Stations, 1983.

[MIL 2002] : MIL STD 882 : System Safety Program for Systems ad associated subsystems and Equipment, 2002.

[MILH 1995]: MIL-HDBK-217, Reliability Prediction for Electronic Components Handbook, 1995.

Sites web intéressants

[ARIA 2006] : http://aria.ecologie.gouv.fr : Brochure de la DRIRE Centre sur la prévention des risques industriels.

http://perso.orange.fr/claude.rochet/systemique.html : THÉORIE ET PRATIQUE DE LA SYSTÉMIQUE ET DE LA COMPLEXITÉ, site personnel de C ROCHET.